日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年　２月　１日

出 願 番 号
Application Number: 特願２０００－０２４５１９

出 願 人
Applicant (s): 富士ゼロックス株式会社

２０００年　７月２１日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号　出証特２０００－３０５６４２１

【書類名】　特許願
【整理番号】　FE00-00023
【提出日】　平成12年 2月 1日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明の名称】　予約証明証発行装置および方法
【請求項の数】　22
【発明者】
【住所又は居所】　神奈川県足柄上郡中井町境４３０　グリーンテクなかい
富士ゼロックス株式会社内
【氏名】　京嶋　仁樹
【発明者】
【住所又は居所】　神奈川県足柄上郡中井町境４３０　グリーンテクなかい
富士ゼロックス株式会社内
【氏名】　申　吉浩
【特許出願人】
【識別番号】　000005496
【氏名又は名称】　富士ゼロックス株式会社
【電話番号】　0462-38-8516
【代理人】
【識別番号】　100086531
【弁理士】
【氏名又は名称】　澤田　俊夫
【電話番号】　03-5541-7577
【手数料の表示】
【予納台帳番号】　038818
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　予約証明証発行装置および方法

【特許請求の範囲】

【請求項１】　物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証を発行する方法であって、

予約証明証の正当性を検証するために必要な検証用情報を作成するステップと、

検証用情報を特定するための情報を入力するステップと、

入力された検証用情報を特定するための情報によって特定される検証用情報で検証可能な予約証明証を作成するステップと、

作成された予約証明証を出力するステップと

を備えていることを特徴とする予約証明証発行方法。

【請求項２】　物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証を発行するコンピュータシステムであって、

予約証明証の正当性を検証するために必要な検証用情報を作成する検証用情報作成手段と、

上記検証用情報作成手段で作成された検証用情報を出力する検証用情報出力手段と、

検証用情報を特定するための情報が入力され、該入力によって特定される検証用情報で検証可能な予約証明証を作成する予約証明証作成手段と、

上記予約証明証作成手段で作成された予約証明証を出力する予約証明証出力手段と

を備えることを特徴とする予約証明証発行システム。

【請求項３】　予約内容を限定するための条件である予約条件を作成する予約条件作成手段を備え、

上記予約証明証作成手段が作成した予約証明証に、上記予約条件作成手段が作成した予約条件が含まれていることを特徴とする

請求項２記載の予約証明証発行システム。

【請求項４】　上記予約証明証作成手段が、

検証用情報を特定するための情報とともに、予約証明証の依頼の仲介者を特定するための情報と、該特定される検証用情報に対応する予約証明証の依頼の仲介が該仲介者に許諾されていることを証明する予約証明証仲介許諾証が入力され、

予約証明証仲介許諾証によって該仲介者に該検証用情報に対応する予約証明証の依頼の仲介が許諾されているかを確認し、許諾されている場合にのみ予約証明証を作成することを特徴とする

請求項２記載の予約証明証発行システム。

【請求項５】　予約証明証の発行履歴を記憶する予約証明証発行履歴記憶部と、

物品やサービスの提供者を特定するための情報の入力を受け、予約証明証発行履歴記憶部に記憶されている発行履歴から、該提供者が提供する物品やサービスに関する予約証明証の発行履歴である予約証明証提供者用発行履歴を抽出する予約証明証提供者用発行履歴作成部と、

前記予約証明証提供者用発行履歴作成部で作成された予約証明証提供者用発行履歴を出力する予約証明証提供者用発行履歴出力部とをさらに備えることを特徴とする

請求項２記載の予約証明証発行システム。

【請求項６】　さらに、予約証明証の発行の依頼を受理する予約証明証発行依頼受理手段を備え、

上記予約証明証発行依頼受理手段が予約証明証発行依頼を受理した場合に、上記予約証明証作成手段で予約証明証を作成し、

予約証明証の発行履歴を記憶する予約証明証発行履歴記憶部と、

予約証明証発行の依頼者を特定するための情報の入力を受け、予約証明証発行履歴記憶部に記憶されている発行履歴から、該依頼者から依頼された予約証明証の発行履歴である予約証明証依頼者用発行履歴を抽出する予約証明証依頼者用発行履歴作成部と、

前記予約証明証依頼者用発行履歴作成部で作成された予約証明証依頼者用発行履歴を出力する予約証明証依頼者用発行履歴出力部とをさらに備えることを特徴

とする

請求項２記載の予約証明証発行システム。

【請求項７】　検証用情報の発行履歴を記憶する検証用情報発行履歴記憶部と、

検証用情報の被発行者を特定するための情報の入力をうけ、検証用情報発行履歴記憶部に記憶されている発行履歴から、該被発行者に対して発行された検証用情報に関する検証用情報の発行履歴である検証用情報発行被発行者用履歴を抽出する検証用情報発行履歴作成部と、

前記検証用情報発行履歴作成部で作成された検証用情報発行被発行者用履歴を出力する検証用情報発行履歴出力部とをさらに備えることを特徴とする

請求項２記載の予約証明証発行システム。

【請求項８】　さらに、公開鍵暗号ペアを作成する公開鍵暗号ペア作成手段と、

上記公開鍵暗号ペア作成手段で作成された公開鍵ペアのうちの秘密鍵を保持する秘密鍵保持手段とを備え、

検証用情報が上記公開鍵暗号ペア作成手段で作成された公開鍵であり、

予約証明証が秘密鍵保持手段に保持されている秘密鍵を使用して作成されることを特徴とする

請求項２記載の予約証明証発行システム。

【請求項９】　物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼を仲介する方法であって、

特定の物品やサービスの提供の予約を証する予約証明証の発行の依頼である第１の予約証明証依頼を受領するステップと、

受領した第１の予約証明証依頼で依頼されている予約証明証の発行を依頼する第２の予約証明証依頼を作成するステップと、

作成された第２の予約証明証依頼を出力するステップと

を有することを特徴とする予約証明証仲介方法。

【請求項１０】　物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼を仲介するコンピュータシステム

であって、

特定の物品やサービスの提供の予約を証する予約証明証の発行の依頼である第１の予約証明証依頼を受領する予約証明証依頼受領手段と、

受領した第１の予約証明証依頼で依頼されている予約証明証の発行を依頼する第２の予約証明証依頼を作成する予約証明証依頼作成手段と、

上記予約証明証依頼作成手段で生成された第２の予約証明証依頼を出力する予約証明証依頼出力手段と

を有することを特徴とする予約証明証仲介システム。

【請求項１１】　特定の予約証明証の正当性を検証するために必要な検証用情報が特定の物品やサービスに対応づけられており、

第１および第２の予約証明証依頼に、該依頼が予約証明証を依頼する物品やサービスを特定するために検証用情報を特定するための情報が含まれる

ことを特徴とする請求項１０記載の予約証明証仲介システム。

【請求項１２】　依頼する予約証明証が予約内容を限定するための条件である予約条件を含むものであり、

依頼する予約証明証に含まれるべき予約条件を作成する予約条件作成手段を備え、

予約証明証依頼作成手段が作成した第２の予約証明証依頼に、上記予約条件作成手段が作成した予約条件が含まれることを特徴とする

請求項１０記載の予約証明証仲介システム。

【請求項１３】　自らが特定の物品やサービスに対する予約証明証の依頼の仲介を許諾されていることを証明する予約証明証仲介許諾証を保持する予約証明証仲介許諾証記憶手段を備え、

予約証明証依頼出力手段が作成する予約証明証依頼に、予約の対象となる物品やサービスに対するものであり、かつ、予約証明証仲介許諾証記憶手段に保持されている予約証明証仲介許諾証を添付することを特徴とする

請求項１０記載の予約証明証仲介システム。

【請求項１４】　さらに、第１の予約証明証依頼の依頼者に予約証明証発行料金の課金を行う課金手段を備え、

第１の予約証明証依頼が入力された時に、上記課金手段によって所定の予約証明証発行料金を該依頼者に対して課金することを特徴とする

請求項１０記載の予約証明証仲介システム。

【請求項１５】　さらに、第１の予約証明証依頼の依頼者から予約証明証発行料金を徴収する決済手段を備え、

第１の予約証明証依頼が入力された時に、上記決済手段によって所定の予約証明証発行料金を該依頼者から徴収することを特徴とする

請求項１０記載の予約証明証仲介システム。

【請求項１６】　物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼の仲介を許諾する方法であって、

物品やサービスの予約証明証の依頼を仲介する仲介者を特定するための情報を入力するステップと、

該仲介者に仲介を許諾する物品やサービスを特定するための情報を入力するステップと、

入力によって特定された物品やサービスに対する予約証明証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する予約証明証仲介許諾証を作成するステップと、

作成された予約証明証仲介許諾証を出力するステップとを有することを特徴とする予約証明証仲介許諾方法。

【請求項１７】　物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼の仲介を許諾するコンピュータシステムであって、

物品やサービスの予約証明証の依頼を仲介する仲介者を特定するための情報と、該仲介者に仲介を許諾する物品やサービスを特定するための情報とが入力され、入力によって特定された物品やサービスに対する予約証明証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する予約証明証仲介許諾証を作成する予約証明証仲介許諾証作成手段と、

上記予約証明証仲介許諾証作成手段で作成された予約証明証仲介許諾証を出力する予約証明証仲介許諾証出力手段と

を有することを特徴とする予約証明証仲介許諾システム。

【請求項１８】　許諾証の受け手である仲介者が仲介することで発行される予約証明証に記載される予約内容を限定するための条件である予約条件の範囲を限定するための情報である予約条件限定情報を作成する予約条件限定情報作成手段を備え、

上記予約証明証仲介許諾証作成手段が作成した予約証明証仲介許諾に、上記予約条件限定情報作成手段が作成した予約条件限定情報が含まれていることを特徴とする

請求項１７記載の予約証明証仲介許諾システム。

【請求項１９】　許諾証の発行履歴を記憶する予約証明証仲介許諾証発行履歴記憶部と、

予約証明証の依頼の仲介者を特定するための情報の入力を受け、予約証明証仲介許諾証発行履歴記憶部に記録されている発行履歴から、該仲介者に対して発行された許諾証に関する履歴である予約証明証仲介許諾証発行仲介者用履歴を抽出する予約証明証仲介許諾証発行仲介者用履歴作成部と、

前記予約証明証仲介許諾証発行仲介者用履歴作成部で作成された予約証明証仲介許諾証発行仲介者用履歴を出力する予約証明証仲介許諾証発行仲介者用履歴出力部とをさらに備えることを特徴とする

請求項１７記載の予約証明証仲介許諾システム。

【請求項２０】　物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の正当性を検証する方法であって、

予約証明証を検証するための検証用情報を記憶するステップと、

予約証明証を入力するステップと、

入力された予約証明証の正当性を記憶した検証用情報を使用して検証するステップと

を有することを特徴とする予約証明証検証方法。

【請求項２１】　物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の正当性を検証する装置であって、

予約証明証を検証するための検証用情報を記憶する検証用情報記憶手段と、

予約証明証が入力され、その予約証明証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する予約証明証検証手段と

を有することを特徴とする予約証明証検証装置。

【請求項２２】　さらに、予約証明証を保持している携帯用記憶装置を接続する接続手段を備え、

予約証明証検証手段が、上記接続手段を通して接続された携帯用記憶装置に記憶されている予約証明証の正当性を検証することを特徴とする

請求項２１記載の予約証明証検証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータシステムにおいて物品あるいはサービスを予約する技術に関わり、特に、消費者が物品あるいはサービスを予約していることを証する予約証明証の発行や、該予約証明証の正当性の検証に関する。

【０００２】

【従来の技術】

特定の場所や特定の時間に限られることの多い物品の取得あるいはサービスの提供を、取得や提供の場所や時間とは独立に許諾する方法として現在もっとも広範に使用されているのは、予約証明証の配布である。

【０００３】

購入希望者が殺到しそうな物品に対して、発売以前に予約を受けつけ、発売時には予約を行った消費者に優先的に物品を発売するという物品の販売方法は非常に広範に行われている。予約済の消費者とそうでない消費者とを区別するために、予約したことを証するものが配布される。この予約証明証は、種々の情報が印刷された紙であったり、あるいは番号であったりする。対価の支払いが物品の引き渡し時に行われる場合もあるし、予約時に行われる場合もある。

【０００４】

サービスの提供では、プレイガイド等のチケット販売業者の窓口で事前に販売される映画やコンサート等の前売り券が最も典型的な例である。この場合には、

情報が紙に印刷されたチケットが予約証明証である。

【０００５】

消費者の家庭にコンピュータが普及し、多くの消費者が日常的にインターネットに接続するようになった昨今では、インターネット上に構築されたサイトで様々な予約が可能になってきた。サイトで予約を依頼したユーザに対して予約証明証にあたるデジタルデータを発行し、物品やサービスの提供時に消費者から発行したデータの提示を受け、予約証明証が正当なものであれば物品やサービスを提供するといったものが典型的な取り引きの方法である。

【０００６】

インターネットを利用した物品やサービスの予約販売は、消費者にとっては、家庭にいながら様々な物品やサービスの予約が可能であるというメリットをもたらした。また、物品やサービスの販売者にとっては物理的な店舗を維持するコストを払うことなく販売経路を拡大できるという利点があり、特に広範な販売店舗網を維持できない小規模な業者にとって、なくてはならない販売経路となりつつある。

【０００７】

【発明が解決しようとする課題】

現在のインターネットを利用した物品やサービスの予約販売は、予約販売業者毎に独立に行われている。各予約販売業者は独自のサイトを運営し、そのサイトで独自の予約証明証を生成し消費者に発行する。各業者は、予約証明証を発行するために必要な開発をそれぞれ独自に行わなければならない上に、予約証明証を発行するサイトの運営コストもそれぞれが負担しなければならない。偽造や複製という危険性を持つ予約証明証というデジタルデータを扱うシステムを運営することは深刻なコストの上昇をもたらし、予約販売業者がインターネットでの予約販売に乗り出す際の重大な障壁になるとともに、販売価格の上昇という不利益を消費者にもたらす。

【０００８】

【課題を解決するための手段】

本発明では、予約販売される特定の物品やサービスあるいは特定の予約販売業

者とは独立の予約証明証の発行を担うサーバ（以降、予約証明証発行センタあるいは単にセンタとよぶ）をインターネット上に構築することで、上記の課題を解決する。予約証明証の作成や維持に関わる部分は予約証明証発行センタがすべて引き受け、物品やサービスの予約販売を行う業者は予約証明証に関わる部分の多くを予約証明証発行センタにアウトソーシングすることができる。多くの予約販売業者が共通の予約証明証発行センタを使用することが可能なので、予約販売業者一つあたりの予約証明証発行センタの開発・運営コストは予約販売業者が独自の予約販売システムを構築するのにくらべて低く押さえることができる。

【０００９】

本発明では、各予約販売業者は、消費者から受けた予約依頼に対して予約証明証を発行するが、その予約証明証は予約証明証発行センタで生成される。予約販売業者は、消費者からの予約の依頼を受け付けるサーバをインターネット上に構築するが、予約証を生成する部分は該サーバ中には存在せず、予約証明証発行センタがその役割を担う。

【００１０】

物品やサービスの提供時には、消費者から予約証明証の提示を受け、予約証明証の正当性が検証されるが、この検証は検証用情報と呼ばれるデジタルデータを使用して行われる。検証用情報は複数の予約証明証との間に所定の関係を満たすように生成されており、検証用情報と予約証明証がその関係を満たすかどうかで予約証明証の正当性が判定される。特定の物品やサービスと特定の検証用情報をバインドさせておけば、その検証用情報と所定の関係を満たす予約証明証を提示できるかどうかで、消費者が正しく予約をしたかどうかが判定できる。

【００１１】

検証用情報は、センタで生成され出力される。どの予約販売業者が販売した予約証明証であっても検証用情報を入手していればその正当性を検証することが可能である。

【００１２】

この特徴は、物品やサービスの予約販売ビジネスをに乗り出す業者が払うべきコストを更に下げる効果を持つ。本発明では、物品やサービスの提供者と、それ

らの予約販売の業者は互いに独立に存立できる。物品やサービスの提供者は、自分が提供する物品やサービスの予約販売を多くの予約販売業者に委託し、自己は物品やサービスの提供に専念することができる。また、予約販売業者は、自らが提供する物品やサービスをまったく持たなくても、様々な提供者が提供する多くの物品やサービスを予約販売する事が可能である。

【００１３】

請求項１または２に記載の発明は予約発行センタに関するものである。

【００１４】

請求項１に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証を発行する方法であって、予約証明証の正当性を検証するために必要な検証用情報を作成するステップと、検証用情報を特定するための情報を入力するステップと、入力された検証用情報を特定するための情報によって特定される検証用情報で検証可能な予約証明証を作成するステップと、作成された予約証明証を出力するステップとを備える。

【００１５】

また、請求項２に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証を発行するコンピュータシステムであって、予約証明証の正当性を検証するために必要な検証用情報を作成する検証用情報作成手段と、上記検証用情報作成手段で作成された検証用情報を出力する検証用情報出力手段と、検証用情報を特定するための情報が入力され、該入力によって特定される検証用情報で検証可能な予約証明証を作成する予約証明証作成手段と、上記予約証明証作成手段で作成された予約証明証を出力する予約証明証出力手段とを備える。

【００１６】

請求項１または２に記載の発明による予約発行センタは、予約証明証を発行するだけでなく、予約証明証を検証するための検証用情報も出力する。この検証用情報は物品やサービスの提供の際に消費者から提示される予約証明証の正当性を検証する際に使用される。特定の検証用情報によって検証可能な予約証明証の集合は限定されるので、特定の物品やサービスに検証用情報を割り当てることで、

物品毎あるいはサービス毎の予約証明証の発行が可能である。しかし、どの検証用情報（あるいはそれに対応する予約証明証の集合）がどの物品やサービスに対応するかに関して予約発行センタは関与する必要はない。特定の物品やサービスと検証用情報との連結は物品やサービスの提供者が自由に決定することができる。このことが、予約証明証発行センタを、特定の物品やサービスに関与しない予約証明証の発行にのみ特化したインフラストラクチャたらしめることを可能にする。

【００１７】

請求項９または１０に記載の発明は、物品やサービスの予約販売を行うサーバに関するものである。

【００１８】

請求項９に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼を仲介する方法であって、特定の物品やサービスの提供の予約を証する予約証明証の発行の依頼である第１の予約証明証依頼を受領するステップと、受領した第１の予約証明証依頼で依頼されている予約証明証の発行を依頼する第２の予約証明証依頼を作成するステップと、作成された第２の予約証明証依頼を出力するステップとを有することを特徴とする。

【００１９】

また、請求項１０に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼を仲介するコンピュータシステムであって、特定の物品やサービスの提供の予約を証する予約証明証の発行の依頼である第１の予約証明証依頼を受領する予約証明証依頼受領手段と、受領した第１の予約証明証依頼で依頼されている予約証明証の発行を依頼する第２の予約証明証依頼を作成する予約証明証依頼作成手段と、上記予約証明証依頼作成手段で生成された第２の予約証明証依頼を出力する予約証明証依頼出力手段とを有することを特徴とする。

【００２０】

請求項９または１０に記載の発明を適用した、物品やサービスの予約販売を行

うサーバは、インターネットに接続している消費者あるいは他の予約販売業者からの予約証明証発行の依頼を受けつける。しかし、受け付けた依頼に対する予約証明証を作成するのはこのサーバではない。予約証明証の発行は予約証明証発行センタのみが行い、物品やサービスの予約販売を行うサーバは、予約証明証発行の仲介のみを行う。該サーバが行うのは、単に依頼の仲介のみであり、予約証明証の改竄、偽造、複製といった攻撃に対する配慮はセンタが行うので、本実施例に基づいた物品やサービスの予約販売を行うサーバの構築費用や運営コストは低く押さえられる。

【００２１】

請求項１６または１７に記載の発明は、物品やサービスの提供者に関するものである。

【００２２】

物品やサービスの提供者と予約販売業者が独立に存立した場合、該提供者にとっては、自己が提供する物品やサービスをより多くの予約販売業者に予約販売をしてもらうほうが、基本的には有利である。しかし、信頼できない予約販売業者に自己の物品やサービスを扱われることは、後のトラブルを招く恐れが高く許容できない。したがって、物品やサービスの提供者が、自己の物品やサービスを扱える予約販売業者を限定できる手段が必要になる。

【００２３】

請求項１６に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼の仲介を許諾する方法であって、物品やサービスの予約証明証の依頼を仲介する仲介者を特定するための情報を入力するステップと、該仲介者に仲介を許諾する物品やサービスを特定するための情報を入力するステップと、入力によって特定された物品やサービスに対する予約証明証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する予約証明証仲介許諾証を作成するステップと、作成された予約証明証仲介許諾証を出力するステップとを有することを特徴とする。

【００２４】

また、請求項１７に記載の発明は、物品やサービスの提供が特定の消費者に対

して予約されていることを証明する電子的な予約証明証の依頼の仲介を許諾するコンピュータシステムであって、物品やサービスの予約証明証の依頼を仲介する仲介者を特定するための情報と、該仲介者に仲介を許諾する物品やサービスを特定するための情報とが入力され、入力によって特定された物品やサービスに対する予約証明証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する予約証明証仲介許諾証を作成する予約証明証仲介許諾証作成手段と、上記予約証明証仲介許諾証作成手段で作成された予約証明証仲介許諾証を出力する予約証明証仲介許諾証出力手段とを有することを特徴とする。

【００２５】

請求項１６または１７に記載の発明によれば、物品やサービスの提供者は、自己が提供する物品やサービスの予約販売を許す予約販売業者に対して予約証明証仲介許諾証を発行する。この予約証明証仲介許諾証は、予約販売業者が予約証明証の発行をセンタに依頼する場合にセンタに対して提示される。センタは提示された予約証明証仲介許諾証により、該予約販売業者が予約証明証の発行を依頼した物品やサービスに対する予約販売を許諾されているかどうかを検査することができる。

【００２６】

請求項２０または２１に記載された発明は、予約証明証の検証に関するものである。

【００２７】

請求項２０に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の正当性を検証する方法であって、予約証明証を検証するための検証用情報を記憶するステップと、予約証明証を入力するステップと、入力された予約証明証の正当性を、記憶した検証用情報を使用して検証するステップとを有することを特徴とする。

【００２８】

また、請求項２１に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の正当性を検証する装置であって、予約証明証を検証するための検証用情報を記憶する検証用情報記憶手

段と、予約証明証が入力され、その予約証明証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する予約証明証検証手段とを有することを特徴とする。

【００２９】

なお、本発明は予約証明証を発行するためにインフラストラクチャを予約販売業者と独立に提供することを可能とするものであるが、副次的に、予約販売業者や、商品やサービスの提供業者と関連する証明証発行センタが、本発明を利用して予約証明証を発行するようにしてもよいことはもちろんである。また、商品やサービスの提供業者が予約販売を直接に行う場合にも本発明の予約証明証発行センタを利用できる。

【００３０】

また、証明証の発行はインターネット以外の通信手段例えば電話回線を利用して行うようにしてもよい。また携帯記録媒体等を用いて機器の間で証明証のやり取りを行うようにしてもよい。

【００３１】

なお、予約は将来商品やサービスの提供を受けたい旨の意思表示であり、商品やサービスを購入してその提供を将来受けるものであればよく、発売日以前の予約のみに限定されない。例えば、ある時点で商品購入の申込を行なうとともに決済を済ませ、数日後にその商品を自宅やコンビニエンスストア等で受け取るというものでもよい。この場合には、申込の証明証あるいは決済ずみの証明証ということもできる。ここでは同じ意味である。

【００３２】

また、履行期が異なる双務的な取引あるいは契約があるときに、一方の債務、例えば金銭の支払が履行されたときにこれを証明する証明証を発行し、反対債務の受給を受けるときにこの証明証で先行債務の履行を証明する場合に、この発明を広く適用できる。

【００３３】

【発明の実施の形態】

以下に、本発明の一実施形態について説明する。

【００３４】

図１は本発明を適用した実施例の構成図である。本実施例は、インターネットに接続した複数のコンピュータシステムからなり、これらが協調して動作することで物品やサービスの予約販売を行う。

【００３５】

本実施例では、消費者は物品やサービスの予約をインターネット経由で行い、予約が完了したことを証するデジタルデータである予約証明証を受け取る。ユーザは受け取った予約証明証をＩＣカード等の携帯型記憶装置に記憶した後、物品やサービスの提供を受ける場所に携行する。消費者が物品やサービスの提供を受ける場所には、予約証明証の検証を行う携帯型記憶装置を接続可能な検証用機器が設置されており、この機器によって予約証明証の正当性が検証されれば、消費者に物品やサービスが提供される。

【００３６】

［実施例を構成するコンピュータシステム群］

本実施例を構成するコンピュータシステムは以下の４つの種類に分類される。それぞれインターネット１０１に接続され、相互に通信を行う。

【００３７】

消費者端末：消費者が物品やサービスの予約を行う際に使用するコンピュータシステム。図１の１０９にあたる。消費者が家庭で使用するコンピュータであってもよいし、コンビニエンスストアに設置されている端末でもよい。インターネット１０１に接続されており、インターネット１０１経由で他のコンピュータシステムにアクセスすることができる。

【００３８】

消費者端末１０９はＩＣカード等の携帯型記憶装置を接続することが可能であり、消費者が持つ携帯型記憶装置１１０が接続され、消費者が取得した予約証明証が携帯型記憶装置１１０に記録される。また、消費者端末と携帯型記憶装置の機能を兼ねるものとして、ノート型のコンピュータや携帯電話を利用してもよい。

【００３９】

図１では、単一の消費者端末のみ図示しているが、インターネットに接続される同様の無数のコンピュータが消費者端末として使用される。

【００４０】

消費者端末を使用する消費者が保持する携帯型記憶装置には、消費者を特定するための識別子である消費者識別子と、消費者自身もその値を知る事ができない秘密情報である消費者秘密情報が格納されている。

【００４１】

消費者識別子と消費者秘密情報のペアはセンタによって保持されており、予約証明証の生成に利用される。

【００４２】

リテーラ：消費者に対して物品やサービスの予約販売を行うコンピュータシステム。図１の１０３あるいは１０４にあたり、実際にはいくつ存在してもかまわない。インターネット１０１に接続されており、インターネット１０１経由で消費者からのアクセスを受け付ける。リテーラを運営しているのは物品やサービスの予約販売をしている業者であるが、以降の本実施例の説明では、該コンピュータシステムと該業者を区別せず、ともにリテーラと呼ぶ事にする。

【００４３】

予約証明証発行センタ：予約証明証を生成し発行するコンピュータシステム。図１の１０２にあたる。インターネット１０１に接続されており、インターネット経由で予約証明証の依頼を受け付け、オンデマンドで予約証明証を作成し発行する。以降、センタといえば予約証明証発行センタを指す。

【００４４】

プロバイダ：物品やサービスの提供者がリテーラ１０３あるいは１０４やセンタ１０２と情報の交換を行うためのコンピュータシステムであり、インターネット１０１に接続される。図１の１０５、１０７にあたり、実際にはいくつ存在してもかまわない。以降の本実施例の説明では、物品やサービスの提供者と該提供者が使用するコンピュータシステムを区別せず、ともにプロバイダと呼ぶ事にする。

【００４５】

認証局（Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ：ＣＡ）：消費者端末、リテーラ、センタ、プロバイダのあいだで交わされる各メッセージには、改竄検知と否認拒否のためにデジタル署名が施される。そのデジタル署名の公開鍵の正当性はＸ．５０９ベースの公開鍵証明証によって保証される。Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ　１１１はこの公開鍵証明証を作成し発行する機能を持つコンピュータシステムであり、インターネット１０１に接続されている。また、Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙは、自己が発行した公開鍵証明証を保持しており、オンデマンドで要求者に送付する機能も持つ。以降、ＣＡといえばＣｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙを指す。

【００４６】

［予約証明証と検証用公開鍵］

本実施例では、消費者が物品やサービスを予約したことを証明するために予約証明証と呼ばれるデジタルデータが発行される。予約証明証の正当性は対応する検証用公開鍵によって検証される。検証用公開鍵の名前が示すように、本実施例では予約証明証と検証用公開鍵には公開鍵暗号技術が応用される。

【００４７】

より具体的には、検証用公開鍵は公開鍵暗号における公開鍵であり、予約証明証は該公開鍵に対応する秘密鍵をもとに作成された予約値を含むデータである。予約証明証が含む予約値を作成する際に使用した秘密鍵と、検証用公開鍵が対応するものであった場合にのみ、予約証明証が正当なものであることが確認でき、それ以外の場合で予約証明証が正当なものであると認められることはない。

【００４８】

本実施例で物品やサービスを予約販売する場合には、予約販売される特定の物品やサービスとバインドされる検証用公開鍵が必要である。特定の検証用公開鍵と特定の物品やサービスをバインドさせることで、特定の物品やサービスにのみ有効な予約証明証を実現することができる。

【００４９】

予約証明証と検証用公開鍵に公開鍵暗号技術を利用しているのは、検証用公開鍵を公開可能とするためである。検証用公開鍵が公開鍵であれば、それを公開し

ても予約証明証の安全性を損なうことがない。このことは、検証用公開鍵の送受信や管理を楽にするだけでなく、予約証明証の正当性を第三者が検証できるようになり、後のトラブルを防ぐことが可能になるという利点がある。

【００５０】

検証用公開鍵はプロバイダからの依頼によって、センタ１０２で作成され、検証用公開鍵情報と呼ばれるデータに含まれて依頼者に送付される。センタ１０２は、検証用公開鍵の発行の要求を受け取ると新しい公開鍵ペアを作成し、その公開鍵と秘密鍵を公開鍵ペアを一意に識別するための情報である検証用公開鍵識別子とともに保持した後、その公開鍵と検証用公開鍵識別子を含む検証用公開鍵情報を依頼者に送付する。検証用公開鍵情報を受け取ったプロバイダを、その検証用公開鍵情報あるいは該検証用公開鍵情報に含まれる検証用公開鍵のユーザと呼ぶ。

【００５１】

特定の検証用公開鍵と特定の物品やサービスのバインドに関してセンタ１０２は関知しない。そのバインドを決定するのは、検証用公開鍵の発行を受けたプロバイダであり、該プロバイダは、自分が決定した特定の物品やサービスと検証用公開鍵とのバインドの情報を保持しておかなければならない。

【００５２】

検証用公開鍵の発行を受けたプロバイダは、該検証用公開鍵に対応する物品やサービスの予約証明証を、検証する機器１０６、１０８に設定する。

【００５３】

消費者はインターネット上でリテーラを介して特定の物品やサービスに対する予約証明証を取得する。取得した予約証明証は、消費者が持つ携帯型記憶装置に記憶される。消費者は物品を入手したりサービスの提供を受けたりする場所に該携帯型記憶装置を持参し、そこにある検証機器１０６、１０８に携帯型記憶装置を接続して予約証明証の正当性の検証を受ける。

【００５４】

物品の予約販売の場合には、物品の引き渡し窓口に予約証明証の検証機器を設置しておき、その検証機器で予約証明証の正当性を検証された消費者のみに物品

を提供する。物品の引き渡し場所は、コンビニエンス・ストアや駅の売店等、検証機器が設置可能な場所であればどこでもよい。

【００５５】

これらの実施形態で消費者に提供される物品は、コンサートや映画の入場券、列車や旅客機への搭乗券、ホテル等の宿泊券等の紙製のチケットの類も含まれる。この場合、コンサートや映画の入場窓口やチケット販売店の窓口、駅や空港の窓口あるいは旅行代理店等に予約証明証の検証機器を設置しておき、そこで予約証明証の正当性を検証した後で引き渡すという実施形態が取れる。

【００５６】

また、検証機器と物品の提供を自動的に連動させた一台の筐体にして、予約証明証の検証後に、自動的に物品が搬出される、自動販売機のような実施形態も取り得る。

【００５７】

また、予約された物品を配達する場合には、配達者が予約証明証を検証する携帯機器を持参し、配達先で物品を引き渡す前に、消費者が所持する予約証明証の正当性を検証し、検証に成功した場合にのみ物品を引き渡すといった方法も可能である。

【００５８】

コンサートや映画の入場といったサービスの提供の場合には、コンサート会場の入場ゲートに予約証明証の検証機能を実装しておき、消費者が入場する際に消費者が持参した予約証明証の正当性を検証して、検証に成功した場合にのみ入場を許すといった実施形態も考えられる。

【００５９】

また、コンサート会場や映画館の特定の座席の使用が提供されるサービスである場合には、該座席に予約証明証の検証機器を付属させ、その座席の検証機器で予約証明証の正当性の検証に成功した消費者のみがこの座席に座ることが許されるように構成すればよい。列車や航空機への入場あるいはその特定の座席の使用といったサービスにおいても同様の方法が利用可能である。

【００６０】

コンサートや映画、列車や航空機の入場あるいは座席指定においては、係員が携帯型の検証器を所持して、各座席を回って座席の使用者が正しい予約証明証を保持することを検証するという実施形態も好適である。

【００６１】

ホテルの部屋の使用というサービスを提供する場合には、ホテルのフロントに検証用機器を置き、それによって予約証明証の正当性を検証する。また、検証用機器を部屋の鍵と連動するように設置し、消費者が持参した予約証明証の検証に成功した場合のみ開錠されるように実装すれば、フロントでの処理を軽減できて効果的である。ロッカー、倉庫等の使用においても同様の実施形態をとることができる。

【００６２】

物品といっても、物理的なものではなく、デジタルデータ等であってもよい。たとえば、インターネット上にある楽曲や画像およびソフトウエア等のデジタルデータのダウンロードの予約に適用することもできる。この場合、検証機器はインターネット上にあるサイトとして実現し、消費者は、家庭にあるＰＣあるいはコンビニ等に設置されている端末から、インターネットを介して検証を行うサイトに予約証明証を提示する。該サイトは、提示された予約証明証の正当性の検証に成功した場合にのみ、消費者にデータのダウンロードを許す。

【００６３】

予約証明証を記憶する携帯型記憶装置としては、記憶機能のみを持つメモリカードやＩＣカード、あるいは計算機能も持つスマートカードなどが利用可能である。接触型あるいは非接触型のどちらでもよい。特に混雑が予想されるコンサート等の入場ゲートに検証用機器を設置する場合には、非接触型のものが望ましい。

【００６４】

携帯電話のように、インターネットに接続可能な端末であってしかも携帯可能なものも好ましい実装の形態である。特に無線での通信機能を持つ携帯型の機器を利用するのは、消費者の利便性も向上し、好適である。

【００６５】

検証用公開鍵情報のデータ構造は以下のようである。

【００６６】

【表１】

検証用公開鍵情報：：＝｛

発行者フィールド，

受領者フィールド，

発行日フィールド，

有効期間開始日時フィールド，

有効期間終了日時フィールド，

検証用公開鍵識別子フィールド，

公開鍵情報フィールド，

デジタル署名フィールド

｝

【００６７】

発行者フィールド：この検証用公開鍵情報の発行者であるセンタの識別子が記載される。

受領者フィールド：この検証用公開鍵情報の受領者であるプロバイダの識別子が記載される。

発行日フィールド：この検証用公開鍵情報の発行日が記載される。

有効期間開始日時フィールド：この検証用公開鍵情報の有効期間の開始日時が記載される。

有効期間終了日時フィールド：この検証用公開鍵情報の有効期間の終了日時が記載される。

検証用公開鍵識別子フィールド：センタがこの検証用公開鍵に割り当てた検証用公開鍵識別子が記載される。

公開鍵情報：予約証明証を検証する際に使用する公開鍵の情報が記載される。使用する公開鍵暗号アルゴリズムの指定と、公開鍵の値を含む。

デジタル署名フィールド：発行者であるセンタによるこの検証用公開鍵情報全体に対するデジタル署名が記載される。

【００６８】

予約証明証のデータ構造は以下のようである。

【００６９】

【表２】

予約証明証：：＝｛

発行者フィールド，

受領者フィールド，

発行日フィールド，

予約証明証識別子フィールド，

公開鍵識別子フィールド，

予約条件フィールド，

予約値フィールド，

デジタル署名フィールド

｝

【００７０】

発行者フィールド：この予約証明証の発行者であるセンタの識別子が記載される。

受領者フィールド：この予約証明証の受領者である消費者の識別子が記載される。

発行日フィールド：この予約証明証の発行日が記載される。

予約証明証識別子フィールド：センタがこの予約証明証に割り当てた識別子が記載される。

公開鍵識別子フィールド：この予約証明証に対応する検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

予約条件フィールド：この予約が有効である範囲を限定する条件である予約条件が記載される。

予約値フィールド：この予約証明証の公開鍵識別子フィールドに記載された識別子が割り当てられた検証用公開鍵に対応する秘密鍵をもとに作成されたデータが記載される。

デジタル署名フィールド：発行者であるセンタによるこの予約証明証全体に対するデジタル署名が記載される。

【００７１】

予約条件には、この予約証明証での予約の有効な範囲を限定するための条件が記載される。

【００７２】

予約条件のデータ構造を以下に示す。

【００７３】

【表３】

予約条件：：＝｛

有効期間開始日時フィールド，

有効期間終了日時フィールド，

・・・

｝

【００７４】

有効期間開始日時フィールド：この予約証明証の有効期間の開始日時が記載される。

有効期間終了日時フィールド：この予約証明証の有効期間の終了日時が記載される。

【００７５】

予約条件に指定された各種条件は、予約証明証の検証時に該条件が満足されているかどうかが検査される。予約条件に指定された各種条件が満足されていなければ、予約証明証の正当性の検証に失敗する。

【００７６】

予約条件には、有効期間の開始日時または終了日時以外にも、予約証明証の用途に応じて種々のものが記載される。

【００７７】

たとえば、その予約証明証がコンサートやイベントの会場あるいは列車や旅客機の特定の座席を予約するものであった場合、その座席番号を予約条件に指定す

れば、該予約条件を含む予約証明証がその座席のみを予約したものであることが証明される。特定のイベントあるいは特定の列車や旅客機のみを予約する場合には、そのイベント名や車番、機番を予約条件に指定すればよい。特定の日時のイベントや搭乗に対する予約であれば、その日付を予約条件に指定する。

【００７８】

また、特定の品名や品番を持つ物品に対する予約であった場合には、その品名や品番を予約条件に指定すればよい。

【００７９】

さらに、物品やサービスの提供時に提供窓口で消費者から料金を徴収する場合、その料金の額をを予約条件に指定し、その料金の額が物品やサービスの提供窓口で支払われた場合にのみ、予約証明証の検証に成功するよう構成することもできる。同様に、値引き額を予約条件に指定したり、物品やサービスの提供時にマイレージ等のポイントを消費者に与える場合には、与えるポイントの高を予約条件に指定することもできる。

【００８０】

また、予約証明証の検証を行う機器や検査者を特定する情報を予約条件に指定し、指定された機器や検査者のみが予約証明証の検証に成功するように構成することもできる。

【００８１】

［予約値］

予約値は予約証明証に含まれるデータである。センタが作成した検証用公開鍵に対応する秘密鍵を元に作成されたデータであり、予約証明証が特定の検証用公開鍵とのみ対応する事を保証するためのものである。また、予約値の作成には、各消費者が持つ秘密情報である消費者秘密情報や、予約証明証に記載された予約条件も使用され、特定の消費者のみが利用可能である事や、特定の予約条件を満足する場合にのみ利用可能である事も保証される。

【００８２】

予約値ｔは法数ｎ、検証用公開鍵ｅ、秘密鍵ｄ、消費者秘密情報ｕ、予約条件ｌから以下の式にしたがって作成される。

【００８３】

【数１】

ｔ＝ｄ－ｆ（ｎ，ｅ，ｕ，ｌ）　　（１）

ここで、関数ｆ（）は公開された一方向性関数である。たとえば、ＳＨＡ－１あるいはＭＤ５等の暗号学的一方向性ハッシュ関数が使用される。

【００８４】

式（１）でわかるように、予約値ｔは、法数ｎ、検証用公開鍵ｅ、消費者秘密情報ｕ、予約条件ｌとともに使用した場合にのみ秘密鍵ｄと同じ働きをする。どれ一つを差し替えても秘密鍵ｄと同じ働きをすることはない。

【００８５】

［予約証明証の検証］

予約証明証の検証は、予約値ｔが秘密鍵ｄと同じ働きができるかどうかを判定する処理である。検証の方法には、いくつかのバリエーションが考えられる。

【００８６】

図２８は、消費者が保持する携帯型記憶装置が演算機能を持っている場合の、該携帯型記憶装置と予約証明証の検証機器の構成例を示した図である。携帯型記憶装置が、スマートカードや携帯電話、あるいはノートＰＣで実現される場合がこれにあたる。

【００８７】

図２８において、２８０１は予約証明証検証機器、２８１１は予約証明証検証機器２８０１に接続される携帯型記憶装置である。予約証明証検証機器２８０１は、チャレンジと呼ぶ乱数値を携帯型記憶装置２８１１に送付し、携帯型記憶装置２８１１は受け取ったチャレンジと保持している予約証明証からレスポンスと呼ぶ値を計算して出力し、予約証明証検証機器２８０１がレスポンスの正しさを検査する事で、携帯型記憶装置２８１１に保持されている予約証明証の正当性を検証する。

【００８８】

予約証明証検証機器２８０１は、条件指定記憶部２８０２、チャレンジ生成部２８０３、公開鍵情報記憶部２８０４、レスポンス検査部２８０５、携帯型記憶

装置制御部２８０６から構成される。

【００８９】

予約証明証検証機器２８０１の各部の役割を以下に示す。

【００９０】

条件指定記憶部２８０２：予約証明証検証機器２８０１が、予約証明証に記載されている予約条件が特定の条件を満たす場合にのみ予約証明証の検証に成功するよう構成する場合、予約条件に関する指定が保持される。

チャレンジ生成部２８０３：携帯型記憶装置２８１１に送付するチャレンジを生成する。

公開鍵情報記憶部２８０４：この予約証明証検証機器に割り当てられた検証用公開鍵の識別子と法数および公開鍵を保持する。

レスポンス検査部２８０５：携帯型記憶装置２８１１が作成したレスポンスの正しさを検査する。

携帯型記憶装置制御部２８０６：携帯型記憶装置２８１１との間の情報のやり取りを制御する。

【００９１】

また、携帯型記憶装置２８１１は入出力制御部２８１２、消費者秘密情報記憶部２８１３、レスポンス計算部２８１４、予約条件判定部２８１５、予約証明証記憶部２８１６から構成される。

【００９２】

携帯型記憶装置２８１１の各部の役割を以下に示す。

【００９３】

入出力制御部２８１２：予約証明証検証機器２８０１との間のデータの入出力を制御する。

消費者秘密情報記憶部２８１３：消費者秘密情報を保持する。

レスポンス計算部２８１４：予約証明証検証機器２８０１に送付するレスポンスを計算する。

予約条件判定部２８１５：予約証明証に記載されている予約条件が満たされているかどうかを判定する。

予約証明証記憶部２８１６：予約証明証が複数保持される。

【００９４】

図２９は、予約証明証の検証の際の予約証明証検証機器２８０１と携帯型記憶装置２８１１の動作を示すフローチャートである。図２９に従って予約証明証の検証の際の予約証明証検証機器２８０１と携帯型記憶装置２８１１の動作を説明する。

【００９５】

予約証明証の検証の動作は予約証明証検証機器２８０１から始まる。

【００９６】

まず、チャンレンジ生成部２８０３でチャレンジＣが作成される（２９０１）。チャンレンジは検証を行うたびに異なる乱数値であり、チャンレンジ生成部２８０３は乱数生成機能を内包している。

【００９７】

チャレンジが生成された後、生成されたチャレンジＣ、公開鍵情報記憶部２８０４に保持されている検証用公開鍵の識別子ＩＤと法数ｎおよび公開鍵ｅ、条件指定記憶部２８０２に保持されている条件指定ｓが、携帯型記憶装置制御部２８０６を介して携帯型記憶装置２８１１に送付される（２９０２）。

【００９８】

Ｃ，ＩＤ，ｎ，ｅ，ｓを受け取った携帯型記憶装置制御部２８０６は、まず予約証明証記憶部２８１６に保持されている予約証明証のうち検証用公開鍵識別子ＩＤに対応するものが選択される（２９０３）。この選択は、予約証明証記憶部２８１６に保持されている予約証明証のうち、その公開鍵識別子フィールドの値がＩＤと等しいかどうかを調べる事で行われる。ここで該当する予約証明証が見つからなければ、エラーが入出力制御部２８１２を介して予約証明証検証機器２８０１に送付され（２９０８）、終了する。

【００９９】

該当する予約証明証が見つかった場合には、予約条件判定部２８１５で該予約証明証に含まれる予約条件１が満たされているかどうかが判定される（２９０４）。予約条件１に記載されている予約証明証の有効期間開始や終了のチェックの

ために、予約条件判定部２８１５は時計を内蔵している。また、予約証明証検証機器２８０１から条件指定ｓが入力されている場合、条件指定ｓが予約条件１を満たすかどうかもここで判定される。たとえば、予約証明証検証機器２８０１がコンサート開場の座席に設置されており、その席の番号を予約条件に持つ予約証明証のみを正当であると判定したい場合には、条件指定として座席番号を条件指定記憶部２８０２に記憶しておき、ｓとして該番号を携帯型記憶装置２８１１に送付し、予約条件判定部２８１５で予約条件１が予約指定ｓに記載されている座席番号を含むかどうかを検査すればよい。

【０１００】

２９０４で、予約条件１が満たされていないと判断された場合、エラーが入出力制御部２８１２を介して予約証明証検証機器２８０１に送付され、終了する（２９０８）。

【０１０１】

２９０４で、予約条件１が満たされていると判断された場合、レスポンス計算部２８１４でレスポンスＲが計算され（２９０５）、入出力制御部２８１２を介して予約証明証検証機器２８０１に送付される（２９０６）。レスポンスＲは、入出力制御部２８１２を介して予約証明証検証機器２８０１から入力されたチャレンジＣ、法数ｎ、公開鍵ｅ、２９０３で選択された予約証明証に含まれる予約値ｔと予約条件１、消費者秘密情報記憶部２８１３に保持されている消費者秘密情報ｕから、以下の（２）式にしたがって計算される。

【０１０２】

【数２】

$$R = C^{t+f(n,e,u,i)} \quad \mathrm{mod} \quad n \qquad (2)$$

携帯型記憶装置制御部２８０６を介してレスポンスＲを受け取った予約証明証検証機器２８０１は、レスポンス検査部２８０５でレスポンスＲの正当性を検証する（２９０７）。検証にはレスポンスＲの他に、チャレンジ生成部２８０３が生成したチャレンジＣ、公開鍵情報記憶部２８０６が記憶している法数ｎ、公開鍵ｅが使用される。（３）の式が成り立てば検証成功、そうでなければ失敗である。

【０１０３】

【数３】

$$C \equiv R^{e} \mod n \qquad (3)$$

（１）（２）（３）の式からわかるように、法数や公開鍵、予約値、予約条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検証に成功する。検証用公開鍵が異なる物品やサービスの予約証明証を流用したり、他人の予約証明証を利用したり、予約条件を改竄したりといった攻撃は困難である。

【０１０４】

図３０は、消費者が保持する携帯型記憶装置が演算機能を持っている場合の、該携帯型記憶装置と予約証明証の検証機器のもう一つの構成例を示した図である。

【０１０５】

図３０において、３００１は予約証明証検証機器、３０１１は予約証明証検証機器３００１に接続される携帯型記憶装置である。予約証明証検証機器３００１は、チャレンジと呼ぶ乱数値を携帯型記憶装置３０１１に送付し、携帯型記憶装置３０１１は受け取ったチャレンジからレスポンスと呼ぶ値を計算して出力し、予約証明証検証機器３００１がレスポンスの正しさを検査する事で、携帯型記憶装置３０１１に保持されている予約証明証の正当性を検証する。図２８の構成では、予約証明証に含まれている予約値や予約条件を使用したのは携帯型記憶装置であったが、図３０の構成では、予約値や予約条件を使用するのは予約証明証検証機器である点が異なる。

【０１０６】

予約証明証検証機器３００１は、チャレンジ生成部３００２、条件指定記憶部３００３、公開鍵情報記憶部３００４、レスポンス検査部３００５、予約条件判定部３００６、予約証明証記憶部３００７、携帯型記憶装置制御部３００８から構成される。

【０１０７】

予約証明証検証機器３００１の各部の役割を以下に示す。

【０１０８】

チャレンジ生成部３００２：携帯型記憶装置３０１１に送付するチャレンジを生成する。

条件指定記憶部３００３：予約証明証検証機器３００１が、予約証明証に記載されている予約条件が特定の条件を満たす場合にのみ予約証明証の検証に成功するよう構成する場合、予約条件に関する指定が保持される。

公開鍵情報記憶部３００４：この予約証明証検証機器に割り当てられた検証用公開鍵の識別子と法数および公開鍵を保持する。

レスポンス検査部３００５：携帯型記憶装置３０１１が作成したレスポンスの正しさを検査する。

予約条件判定部３００６：予約証明証に記載されている予約条件が満たされているかどうかを判定する。

予約証明証記憶部３００７：携帯型記憶装置３０１１から取り出した予約証明証を保持する。

携帯型記憶装置制御部３００８：携帯型記憶装置３０１１との間の情報のやり取りを制御する。

【０１０９】

また、携帯型記憶装置３０１１は、入出力制御部３０１２、消費者秘密情報記憶部３０１３、レスポンス計算部３０１４、予約証明証記憶部３０１５から構成される。

【０１１０】

携帯型記憶装置３０１１の各部の役割を以下に示す。

【０１１１】

入出力制御部３０１２：予約証明証検証機器３００１との間のデータの入出力を制御する。

消費者秘密情報記憶部３０１３：消費者秘密情報を保持する。

レスポンス計算部３０１４：予約証明証検証機器３００１に送付するレスポンスを計算する。

予約証明証記憶部３０１５：予約証明証が複数保持される。

【０１１２】

図３１は、予約証明証の検証の際の予約証明証検証機器３００１と携帯型記憶装置３０１１の動作を示すフローチャートである。図３１に従って予約証明証の検証の際の予約証明証検証機器３００１と携帯型記憶装置３０１１の動作を説明する。

【０１１３】

予約証明証の検証の動作は予約証明証検証機器３００１から始まる。

【０１１４】

予約証明証検証機器３００１は、携帯型記憶装置制御部３００８を介して携帯型記憶装置３０１１の予約証明証記憶部３０１５にアクセスし、予約証明証記憶部３０１５に保持されている予約証明証のうち、予約証明証検証機器３００１による予約証明証検証に使用可能なものを探す（３１０１）。予約証明証記憶部３０１５に保持されている予約証明証のうち、その公開鍵識別子フィールドの値が公開鍵情報記憶部３００４に保持されている検証用公開鍵識別子と一致するものが、求める予約証明証である。ここで該当する予約証明証が見つからなければ、予約証明証の検証は失敗であり、エラー処理の後（３１０９）、終了する。

【０１１５】

該当する予約証明証が見つかった場合には、該予約証明証が取り出され、予約証明証検証機器３００１の予約証明証記憶部３００７に記憶される（３１０２）。

【０１１６】

次に、予約条件判定部３００６で、予約証明証記憶部３００７に保持されている予約証明証に含まれる予約条件１が満たされているかどうかが判定される（３１０３）。予約条件１に記載されている予約証明証の有効期間開始や終了のチェックのために、予約条件判定部３００６は時計を内蔵している。また、条件指定記憶部３００３に条件指定が保持されている場合、該条件指定が予約条件１を満たすかどうかもここで判定される。たとえば、予約証明証検証機器３００１がホテルの部屋のドアに設置されており、その部屋番号を予約条件に持つ予約証明証のみを正当であると判定したい場合には、条件指定として部屋番号を条件指定記憶部３００３に記憶しておき、予約条件判定部３００６で予約条件１が条件指定

記憶部３００３に保持されている部屋番号を含むかどうかを検査すればよい。

【０１１７】

３１０３で、予約条件１が満たされていないと判断された場合、予約証明証の検証は失敗であり、エラー処理の後（３１０９）、終了する。

【０１１８】

３１０３で、予約条件１が満たされていると判断された場合、チャレンジ生成部３００２でチャレンジＣが作成される（３１０４）。チャンレンジは検証を行うたびに異なる乱数値であり、チャンレンジ生成部３００２は乱数生成機能を内包している。

【０１１９】

チャレンジが生成された後、生成されたチャレンジＣ、公開鍵情報記憶部３００４に保持されている法数ｎおよび公開鍵ｅ、予約証明証記憶部３００７に記憶されている予約証明証が含む予約条件１が、携帯型記憶装置制御部３００８を介して携帯型記憶装置３０１１に送付される（３１０５）。

【０１２０】

チャレンジを受け取った携帯型記憶装置３０１１は、レスポンス計算部３０１４でレスポンスＲを計算し（３１０６）、入出力制御部３０１２を介して予約証明証検証機器３００１に送付される（３１０７）。レスポンスＲは、入出力制御部３０１２を介して予約証明証検証機器３００１から入力されたチャレンジＣ、法数ｎ、公開鍵ｅ、予約条件１、消費者秘密情報記憶部３０１３に保持されている消費者秘密情報ｕから、以下の（４）式にしたがって計算される。

【０１２１】

【数４】

$$R = C^{f(n,e,u,l)} \mod n \qquad (4)$$

携帯型記憶装置制御部３００８を介してレスポンスＲを受け取った予約証明証検証機器３００１は、レスポンス検査部３００５でレスポンスＲの正当性を検証する（３１０８）。検証にはレスポンスＲの他に、チャレンジ生成部３００２が生成したチャレンジＣ、公開鍵情報記憶部３００４が記憶している法数ｎ、公開鍵ｅ、予約証明証記憶部３００７が保持している予約証明証に含まれる予約値ｔが

使用される。（５）の式が成り立てば検証成功、そうでなければ失敗である。

【０１２２】

【数５】

$$C \equiv (C^{t}R)^{e} \mod n \qquad (5)$$

（１）（４）（５）の式からわかるように、法数や公開鍵、予約値、予約条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検証に成功する。検証用公開鍵が異なる物品やサービスの予約証明証を流用したり、他人の予約証明証を利用したり、予約条件を改竄したりといった攻撃は困難である。

【０１２３】

図３２は、消費者が保持する携帯型記憶装置が演算機能を持っていない場合の、該携帯型記憶装置と予約証明証の検証機器の構成例を示した図である。

【０１２４】

図３２において、３２０１は予約証明証検証機器、３２１１は予約証明証検証機器３２０１に接続される携帯型記憶装置である。予約証明証検証機器３２０１は、携帯型記憶装置３２１１が保持している予約証明証をとりだし、その正当性を検証する。

【０１２５】

予約証明証検証機器３２０１は、条件指定記憶部３２０２、予約条件判定部３２０３、公開鍵情報記憶部３２０４、予約値検査部３２０５、予約証明証記憶部３２０６、携帯型記憶装置制御部３２０７、消費者秘密情報記憶部３２０８から構成される。

【０１２６】

予約証明証検証機器３２０１の各部の役割を以下に示す。

【０１２７】

条件指定記憶部３２０２：予約証明証検証機器３２０１が、予約証明証に記載されている予約条件が特定の条件を満たす場合にのみ予約証明証の検証に成功するよう構成する場合、予約条件に関する指定が保持される。

予約条件判定部３２０３：予約証明証に記載されている予約条件が満たされているかどうかを判定する。

公開鍵情報記憶部３２０４：この予約証明証検証機器に割り当てられた検証用公開鍵の識別子と法数および公開鍵を保持する。

予約値検査部３２０５：予約証明証に記載されている予約値の正当性を検証する。

予約証明証記憶部３２０６：携帯型記憶装置３２１１から取り出した予約証明証を保持する。

携帯型記憶装置制御部３２０７：携帯型記憶装置３２１１との間の情報のやり取りを制御する。

消費者秘密情報記憶部３２０８：携帯型記憶装置３２１１から取り出した消費者秘密情報を保持する。

【０１２８】

また、携帯型記憶装置３２１１は、入出力制御部３２１２、消費者秘密情報記憶部３２１３、予約証明証記憶部３２１４から構成される。

【０１２９】

携帯型記憶装置３２１１の各部の役割を以下に示す。

【０１３０】

入出力制御部３２１２：予約証明証検証機器３２０１との間のデータの入出力を制御する。

消費者秘密情報記憶部３２１３：消費者秘密情報を保持する。

予約証明証記憶部３２１４：予約証明証が複数保持される。

【０１３１】

図３３は、予約証明証の検証の際の予約証明証検証機器３２０１と携帯型記憶装置３２１１の動作を示すフローチャートである。図３３に従って予約証明証の検証の際の予約証明証検証機器３２０１と携帯型記憶装置３２１１の動作を説明する。

【０１３２】

予約証明証検証機器３２０１は、携帯型記憶装置制御部３２０７を介して携帯型記憶装置３２１１の予約証明証記憶部３２１４にアクセスし、予約証明証記憶部３２１４に保持されている予約証明証のうち、予約証明証検証機器３２０１に

よる予約証明証検証に使用可能なものを探す（３３０１）。予約証明証記憶部３２１４に保持されている予約証明証のうち、その公開鍵識別子フィールドの値が公開鍵情報記憶部３２０４に保持されている検証用公開鍵識別子と一致するものが、求める予約証明証である。ここで該当する予約証明証が見つからなければ、予約証明証の検証は失敗であり、エラー処理の後（３３０６）、終了する。

【０１３３】

該当する予約証明証が見つかった場合には、該予約証明証が取り出され、予約証明証検証機器３２０１の予約証明証記憶部３２０６に記憶される（３３０２）。

【０１３４】

次に、予約条件判定部３２０３で、予約証明証記憶部３２０６に保持されている予約証明証に含まれる予約条件１が満たされているかどうかが判定される（３３０３）。予約条件１に記載されている予約証明証の有効期間開始や終了のチェックのために、予約条件判定部３２０３は時計を内蔵している。また、条件指定記憶部３２０３に条件指定が保持されている場合、該条件指定が予約条件１を満たすかどうかもここで判定される。

【０１３５】

３３０３で、予約条件１が満たされていないと判断された場合、予約証明証の検証は失敗であり、エラー処理の後（３３０６）、終了する。

【０１３６】

３３０３で、予約条件１が満たされていると判断された場合、携帯型記憶装置制御部３２０７を介して携帯型記憶装置３２１１の消費者秘密情報記憶部３２１３にアクセスし、消費者秘密情報記憶部３２１３に保持されている消費者秘密情報ｕを取り出し、予約証明証検証機器３２０１の消費者秘密情報記憶部３２０８に記憶する（３３０４）。

【０１３７】

最後に、予約値検査部３２０５で、予約証明証記憶部３２０６に保持されている予約証明証に含まれる予約値ｔの正当性を検証する（３３０５）。検証のために、予約値検査部３２０５は乱数ｒを生成し、公開鍵情報記憶部３２０４が記憶

している法数ｎ、公開鍵ｅ、予約証明証記憶部３２０６が保持している予約証明証に含まれる予約条件１、消費者秘密情報記憶部３２０８が保持している消費者秘密情報ｕに対して　（６）の式が成り立つかどうかを検査する。

【０１３８】

【数６】

$$r \equiv (r^{t+f(n,e,u,l)})^{e} \mod n \qquad (6)$$

（１）（６）の式からわかるように、法数や公開鍵、予約値、予約条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検証に成功する。検証用公開鍵が異なる物品やサービスの予約証明証を流用したり、他人の予約証明証を利用したり、予約条件を改竄したりといった攻撃は困難である。

【０１３９】

［検証用公開鍵情報の発行］

検証用公開鍵情報はプロバイダからの依頼によって、センタで作成され、依頼したプロバイダに送付される。依頼の際には、検証用公開鍵情報依頼というデータが送受信される。通常、発信者は依頼をするプロバイダであり受信者は依頼を受けるセンタであるが、インターネットに接続されたその他のエンティティがプロバイダの代わりに依頼を行ったりセンタの代わりに依頼を受けたりする場合には、プロバイダやセンタ以外のエンティティが発信者や受信者になってもよい。

【０１４０】

検証用公開鍵情報依頼のデータ構造を以下に示す。

【０１４１】

【表４】

検証用公開鍵情報依頼：：＝｛

発信者フィールド，
受信者フィールド，
日時フィールド，
公開鍵仕様フィールド，
デジタル署名フィールド，
証明証フィールド

}

【０１４２】

発信者フィールド：この検証用公開鍵情報依頼の発信者の識別子が記載される。発信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この検証用公開鍵情報依頼の受信者の識別子が記載される。受信者は通常予約証発行センタであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この検証用公開鍵情報依頼の作成日時が記載される。

公開鍵仕様フィールド：作成してもらう検証用公開鍵に対する依頼者の要望が記載される。検証用公開鍵を使用するプロバイダの識別子、公開鍵暗号アルゴリズム、鍵長の情報がここに記述できる。

デジタル署名フィールド：この検証用公開鍵情報依頼の発信者によるこの検証用公開鍵情報依頼に対するデジタル署名が記載される。

証明証フィールド：この検証用公開鍵情報依頼のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０１４３】

検証用公開鍵情報依頼を受け取ったセンタは、検証用公開鍵情報依頼に記載された公開鍵仕様にしたがって公開鍵ペアを作成し、検証用公開鍵情報を作成して依頼者であるプロバイダに渡す。依頼された検証用公開鍵情報を作成するかしないか、あるいは、指定された公開鍵仕様通りに公開鍵を作成するかどうかはセンタが決定できる。

【０１４４】

検証用公開鍵情報を引き渡す際には、検証用公開鍵情報送付というデータが送受信される。通常、発信者は検証用公開鍵情報を作成したセンタであり、受信者は発行された検証用公開鍵情報を使用するプロバイダであるが、インターネットに接続されたその他のエンティティがセンタの代わりに検証用公開鍵情報の送付を行ったり、プロバイダの代わりに検証用公開鍵情報を受け取ったりする場合には、センタやプロバイダ以外のエンティティが発信者や受信者になってもよい。

【０１４５】

検証用公開鍵情報送付のデータ構造を以下に示す。

【０１４６】

【表５】

検証用公開鍵情報送付：：＝｛

発信者フィールド，
受信者フィールド，
日時フィールド，
検証用公開鍵情報フィールド，
デジタル署名フィールド，
証明証フィールド

｝

【０１４７】

発信者フィールド：この検証用公開鍵情報送付の送付者の識別子が記載される。発信者は通常予約証発行センタであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この検証用公開鍵情報送付の受信者の識別子が記載される。受信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この検証用公開鍵情報送付の作成日時が記載される。

検証用公開鍵情報フィールド：この検証用公開鍵情報送付で送られる検証用公開鍵情報が記載される。

デジタル署名フィールド：この検証用公開鍵情報送付の発信者によるこの検証用公開鍵情報送付に対するデジタル署名が記載される。

証明証フィールド：この検証用公開鍵情報送付のデジタル署名フィールド、およびこの検証用公開鍵情報送付に含まれる検証用公開鍵情報のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０１４８】

［予約証明証仲介許諾］

本実施例では、プロバイダとリテーラは独立に存立することが可能である。リテーラは多様なプロバイダが提供する多様な物品やサービスの予約販売を行うことが可能であるし、特定のプロバイダが自己の提供する物品やサービスを多くのリテーラに予約販売をしてもらうといったことも可能である。

【０１４９】

プロバイダにとっては、多くのリテーラに自己の商品を予約販売してもらうことは基本的には有利であるが、自分と取引のない信用度の低いリテーラに予約販売をされるのは、後のトラブルを招く可能性が高く許容できない。したがって、プロバイダは自己の物品やサービスを取り扱えるリテーラをコントロールする必要がある。

【０１５０】

このコントロール可能にするために、本実施例では予約証明証仲介許諾というデータを使用する。

【０１５１】

予約証明証仲介許諾はプロバイダが特定のリテーラに対して自己の特定の物品やサービスの予約販売を委託している事を証するデジタルデータであり、リテーラからの依頼を受けて作成され、依頼者に送付される。

【０１５２】

予約証明証仲介許諾のデータ構造を以下に示す。

【０１５３】

【表６】

予約証明証仲介許諾：：＝｛

発行者フィールド，
受領者フィールド，
発行日フィールド，
予約証明証仲介許諾識別子フィールド，
有効期間開始日時フィールド，
有効期間終了日時フィールド，

公開鍵鍵識別子フィールド，
予約条件限定情報フィールド，
デジタル署名フィールド
｝

【０１５４】

発行者フィールド：この予約証明証仲介許諾の発行者であるプロバイダの識別子が記載される。

受領者フィールド：この予約証明証仲介許諾の受領者であるリテーラの識別子が記載される。

発行日フィールド：この予約証明証仲介許諾の発行日が記載される。

予約証明証仲介許諾識別子フィールド：この予約証明証仲介許諾にプロバイダが割り当てた識別子が記載される。

有効期間開始日時フィールド：この予約証明証仲介許諾の有効期間の開始日時が記載される。

有効期間終了日時フィールド：この予約証明証仲介許諾の有効期間の終了日時が記載される。

公開鍵識別子フィールド：この予約証明証仲介許諾によって予約証明証の仲介が許諾される検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

予約条件限定情報フィールド：予約証明証に記載される予約条件の範囲を限定する情報である予約条件限定情報が記載される。

デジタル署名フィールド：発行者であるプロバイダによるこの予約証明証仲介許諾全体に対するデジタル署名が記載される。

【０１５５】

予約条件限定情報フィールドに記載される予約条件限定情報によって、プロバイダはリテーラが発行する予約証明証に記載される予約条件を詳細にコントロールする事ができる。

【０１５６】

予約条件限定情報のデータ構造を以下に示す。

【０１５７】

【表７】

予約条件限定情報：：＝｛

最短有効期間フィールド，

最長有効期間フィールド，

・・・

｝

【０１５８】

最短有効期間フィールド：この予約証明証仲介許諾の受領者であるリテーラが仲介して発行される、公開鍵鍵識別子で指定された検証用公開鍵に対応する予約証明証の予約条件フィールドに記載される有効期間開始から有効期間終了までの間の長さの最低限度が記載される。該予約証明証の予約条件フィールドに記載される有効期間開始から有効期間終了までの間の長さは、ここに記載される値以上でなければならない。

最長有効期間フィールド：この予約証明証仲介許諾の受領者であるリテーラが仲介して発行される、公開鍵鍵識別子で指定された検証用公開鍵に対応する予約証明証の予約条件フィールドに記載される有効期間開始から有効期間終了までの間の長さの最長限度が記載される。該予約証明証の予約条件フィールドに記載される有効期間開始から有効期間終了までの間の長さは、ここに記載される値以下でなければならない。

【０１５９】

予約条件限定情報には、最短有効期間あるいは最長有効期間以外にも、この予約証明証仲介許諾の公開鍵鍵識別子フィールドで指定された検証用公開鍵とバインドされている物品やサービスに応じて種々の限定を設定する事が可能である。たとえば、公開鍵鍵識別子フィールドで指定された検証用公開鍵が特定の日時のコンサートでの座席の予約に対応するものであって、特定のリテーラが予約販売できる座席を限定したい場合には、予約販売を許す座席番号の集合を予約条件限定情報フィールドに記載すればよい。これにより、予約証明証の予約条件フィールドに記載される座席番号を限定する事ができる。

【０１６０】

［予約証明証仲介許諾の発行］

予約証明証仲介許諾はリテーラからの依頼によって、プロバイダで作成され、依頼したリテーラに送付される。依頼の際には、予約証明証仲介許諾依頼というデータが送受信される。通常、発信者は依頼をするリテーラであり受信者は依頼を受けるプロバイダであるが、インターネットに接続されたその他のエンティティがリテーラの代わりに依頼を行ったりプロバイダの代わりに依頼を受けたりする場合には、リテーラやプロバイダ以外のエンティティが発信者や受信者になってもよい。

【０１６１】

予約証明証仲介許諾依頼のデータ構造を以下に示す。

【０１６２】

【表８】

予約証明証仲介許諾依頼：：＝｛

発信者フィールド，
受信者フィールド，
日時フィールド，
予約証明証仲介許諾仕様フィールド，
デジタル署名フィールド，
証明証フィールド
｝

【０１６３】

発信者フィールド：この予約証明証仲介許諾依頼の発信者の識別子が記載される。発信者は通常リテーラであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この予約証明証仲介許諾依頼の受信者の識別子が記載される。受信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この予約証明証仲介許諾依頼の作成日時が記載される。

予約証明証仲介許諾仕様フィールド：作成してもらう予約証明証仲介許諾に対す

る依頼者の要望を記載した予約証明証仲介許諾仕様が記載される。

デジタル署名フィールド：この予約証明証仲介許諾依頼の発信者によるこの予約証明証仲介許諾依頼に対するデジタル署名が記載される。

証明証フィールド：この予約証明証仲介許諾依頼のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０１６４】

予約証明証仲介許諾依頼の予約証明証仲介許諾仕様フィールドに記載される予約証明証仲介許諾仕様のデータ構造を以下に示す。

【０１６５】

【表９】

予約証明証仲介許諾仕様：：＝｛

許諾者フィールド，

被許諾者フィールド，

公開鍵識別子フィールド，

希望予約条件限定情報フィールド

｝

【０１６６】

許諾者フィールド：予約証明証仲介許諾を作成してほしいプロバイダの識別子が記載される。

被許諾者フィールド：希望する予約証明証仲介許諾によって許諾を受けるリテーラの識別子が記載される。

公開鍵鍵識別子フィールド：予約証明証仲介許諾で予約証明証の仲介を許諾してほしい検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

希望予約条件限定情報フィールド：作成してもらう予約証明証仲介許諾に記載してほしい予約条件限定情報が記載される。

【０１６７】

予約証明証仲介許諾依頼を受け取ったプロバイダは、予約証明証仲介許諾依頼に記載された予約証明証仲介許諾仕様にしたがって予約証明証仲介許諾を作成し、リテーラに渡す。依頼された予約証明証仲介許諾を作成するかしないか、ある

いは、指定された予約証明証仲介許諾仕様どおりに予約証明証仲介許諾を作成するかどうかはプロバイダが決定できる。

【０１６８】

作成した予約証明証仲介許諾を引き渡す際には、予約証明証仲介許諾送付というデータが送受信される。通常、発信者は予約証明証仲介許諾を作成したプロバイダであり、受信者は発行された予約証明証仲介許諾を使用するリテーラであるが、インターネットに接続されたその他のエンティティがプロバイダの代わりに予約証明証仲介許諾の送付を行ったり、リテーラの代わりに予約証明証仲介許諾を受け取ったりする場合には、プロバイダやリテーラ以外のエンティティが発信者や受信者になってもよい。

【０１６９】

予約証明証仲介許諾送付のデータ構造を以下に示す。

【０１７０】

【表１０】

予約証明証仲介許諾送付：：＝｛

発信者フィールド，
受信者フィールド，
日時フィールド，
予約証明証仲介許諾フィールド，
デジタル署名フィールド，
証明証フィールド
｝

【０１７１】

発信者フィールド：この予約証明証仲介許諾送付の送付者の識別子が記載される。発信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この予約証明証仲介許諾送付の受信者の識別子が記載される。受信者は通常リテーラであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この予約証明証仲介許諾送付の作成日時が記載される。
予約証明証仲介許諾フィールド：この予約証明証仲介許諾送付で送られる予約証明証仲介許諾が記載される。
デジタル署名フィールド：この予約証明証仲介許諾送付の発信者によるこの予約証明証仲介許諾送付に対するデジタル署名が記載される。
証明証フィールド：この予約証明証仲介許諾送付のデジタル署名フィールド、およびこの予約証明証仲介許諾送付に含まれる予約証明証仲介許諾のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０１７２】

［予約証明証の発行］

予約証明証は、消費者からの依頼に応じて発行される。消費者はリテーラに対して特定の物品やサービスに対して特定の予約条件での予約を依頼する予約証明証依頼を送付する。予約証明証依頼を受け取ったリテーラは、通常センタに対して、依頼元である消費者に対する予約証明証の発行を依頼するため予約証明証依頼を作成し、センタに送付する。予約証明証依頼を受け取ったセンタは消費者向けの予約証明証を作成し、予約証明証依頼を送付してきたリテーラに渡す。予約証明証を受け取ったリテーラは、その予約証明証をその依頼者である消費者に送付する。センタからあるいはリテーラからの予約証明証の送付には、予約証明証送付というデータが送受信される。

【０１７３】

消費者とセンタの間を複数のリテーラが仲介することも可能である。その場合、消費者からの依頼を直接受けたリテーラが第２のリテーラに予約証明証依頼を送付し、第２のリテーラがセンタに予約証明証依頼を送付するという形態をとる。発行された予約証明証は逆の経路で予約証明証送付を送付していく事で消費者に届く。

【０１７４】

予約証明証依頼のデータ構造を以下に示す。

【０１７５】

【表１１】

予約証明証依頼：：＝｛

発信者フィールド，

受信者フィールド，

日時フィールド，

予約内容フィールド，

デジタル署名フィールド，

証明証フィールド

｝

【０１７６】

発信者フィールド：この予約証明証依頼の発信者の識別子が記載される。

受信者フィールド：この予約証明証依頼の受信者の識別子が記載される。

日時フィールド：この予約証明証依頼の作成日時が記載される。

予約内容フィールド：依頼する予約証明証の内容に関する要望のためのフィールドである。通常、予約内容に関する要望を記した予約仕様が記載されるが、受信者がリテーラであって、リテーラで予約販売している物品あるいはサービスにリテーラ独自の管理番号が割り当ててある場合には、その番号が記載されることもある。

デジタル署名フィールド：この予約証明証依頼の発信者によるこの予約証明証依頼に対するデジタル署名が記載される。

証明証フィールド：この予約証明証依頼のデジタル署名フィールド、およびこの予約証明証依頼に予約証明証仲介許諾が含まれるならばそのデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０１７７】

予約証明証依頼の予約内容フィールドに記載される予約仕様のデータ構造を以下に示す。

【０１７８】

【表１２】

予約仕様　　：：＝｛

公開鍵識別子フィールド，

消費者識別子フィールド，

予約条件フィールド，

予約証明証仲介許諾フィールド

｝

【０１７９】

公開鍵鍵識別子フィールド：予約証明証依頼で依頼する予約証明証を検証できる検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

消費者識別子フィールド：予約証明証依頼で依頼する予約証明証で予約を証される消費者の識別子が記載される。

予約条件フィールド：予約証明証依頼で依頼する予約証明証に記載してほしい予約条件が記載あされる。

予約証明証仲介許諾フィールド：予約証明証依頼の発信者がリテーラの場合に、そのリテーラが、この予約仕様の公開鍵鍵識別子フィールドに指定された識別子をもつ検証用公開鍵に対応する予約証明証を、この予約仕様の予約条件フィールドに記載された予約条件で依頼することの仲介が許諾されている事を証する予約証明証仲介許諾が含まれる。

【０１８０】

予約仕様の予約条件フィールドに記載されたとおりの予約条件を持つ予約証明証を発行するかどうかは、センタが決定する。特に、予約仕様に含まれる予約証明証仲介許諾で許諾されていない依頼に対しては、予約証明証を発行しない。

【０１８１】

また、予約証明証の依頼の過程で、仲介するリテーラが予約仕様の予約条件フィールドの内容を修正する事もありうる。

【０１８２】

予約証明証送付のデータ構造を以下に示す。

【０１８３】

【表１３】

予約証明証送付：：＝｛

発信者フィールド，

受信者フィールド，

日時フィールド，

予約証明証フィールド，

デジタル署名フィールド，

証明証フィールド

｝

【０１８４】

発信者フィールド：この予約証明証送付の送付者の識別子が記載される。

受信者フィールド：この予約証明証送付の受信者の識別子が記載される。

日時フィールド：この予約証明証送付の作成日時が記載される。

予約証明証フィールド：この予約証明証送付で送られる予約証明証が記載される。

デジタル署名フィールド：この予約証明証送付の発信者によるこの予約証明証仲介許諾送付に対するデジタル署名が記載される。

証明証フィールド：この予約証明証送付のデジタル署名フィールド、およびこの予約証明証送付に含まれる予約証明証のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【０１８５】

［センタの構成］

本実施例のセンタは、インターネットを介して入力される検証用公開鍵情報依頼と予約証明証依頼を処理する機能、予約証明証の発行履歴を作成してインターネットを介してプロバイダあるいはリテーラに送付する機能、検証用公開鍵情報の発行履歴を作成してインターネットを介してプロバイダに送付する機能を持つ。

【０１８６】

図２は、本実施例のセンタの構成図である。

【０１８７】

センタは、入出力制御部２０１、処理選択部２０２、検証用公開鍵情報依頼処理部２０３、予約証明証依頼処理部２０４、プロバイダＤＢ２０５、公開鍵ペアＤＢ２０６、リテーラＤＢ２０７、消費者ＤＢ２０８、予約証明証発行履歴ＤＢ２０９、署名鍵記憶部２１０、証明証記憶部２１１、予約証明証発行プロバイダ用履歴作成部２１２、予約証明証発行リテーラ用履歴作成部２１３、検証用公開鍵情報発行履歴作成部２１４から構成され、入出力制御部２０１を介してインターネットに接続されている。

【０１８８】

本実施例のセンタの各部の役割を以下に述べる。

【０１８９】

入出力制御部２０１：インターネットを介したデータの入力を受け付けるとともに、検証用公開鍵情報依頼処理部２０３が作成したデータや予約証明証依頼処理部２０４が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部２０１への入力、あるいは、入出力制御部２０１からインターネットへの出力の方法としては、入出力制御部２０１と接続されたＷＷＷサイトを準備してプロバイダやリテーラにアクセスさせるもの、あるいは電子メールシステムと入出力制御部２０１を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部２０２：入力したデータが検証用公開鍵情報依頼かまたは予約証明証依頼かを判断し、検証用公開鍵情報依頼であれば検証用公開鍵情報依頼処理部２０３を、予約証明証依頼であれば予約証明証依頼処理部２０４を呼び出す。

検証用公開鍵情報依頼処理部２０３：検証用公開鍵情報依頼を処理し、検証用公開鍵情報依頼送付を作成して入出力制御部２０１を介して依頼者に送付する。検証用公開鍵情報依頼送付作成の過程で、プロバイダＤＢ２０５を参照するとともに、公開鍵ペアＤＢ２０６に新しいエントリを追加する。

予約証明証依頼処理部２０４：予約証明証依頼を処理し、予約証明証依頼送付を作成して入出力制御部２０１を介して依頼者に送付する。予約証明証依頼送付作成の過程で、公開鍵ペアＤＢ２０６、リテーラＤＢ２０７、消費者ＤＢ２０８を参照するとともに、予約証明証発行履歴ＤＢに新しいエントリを追加する。

プロバイダＤＢ２０５：プロバイダに関するデータを保持するＤＢ。
公開鍵ペアＤＢ２０６：検証用公開鍵情報あるいは予約証明証の作成に使用される公開鍵ペアを保持するＤＢ。
リテーラＤＢ２０７：リテーラに関するデータを保持するＤＢ。
消費者ＤＢ２０８：消費者に関するデータを保持するＤＢ。
予約証明証発行履歴ＤＢ２０９：予約証明証の発行履歴に関するデータを保持するＤＢ。
署名鍵記憶部２１０：センタが作成するデジタル署名に使用する署名鍵を保持する。
証明証記憶部２１１：署名鍵記憶部２１０に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。
予約証明証発行プロバイダ用履歴作成部２１２：各プロバイダ毎の予約証明証の発行履歴を作成し、入出力制御部２０１を介してプロバイダに送付する。
予約証明証発行リテーラ用履歴作成部２１３：各リテーラ毎の予約証明証の発行履歴を作成し、入出力制御部２０１を介してリテーラに送付する。
検証用公開鍵情報発行履歴作成部２１４：各プロバイダ毎の検証用公開鍵情報の発行履歴を作成し、入出力制御部２０１を介してプロバイダに送付する。

【０１９０】

［センタが持つデータベース］

センタは、プロバイダＤＢ２０５、公開鍵ペアＤＢ２０６、リテーラＤＢ２０７、消費者ＤＢ２０８、予約証明証発行履歴ＤＢ２０９の５つのデータベースを持っている。

【０１９１】

プロバイダＤＢ２０５は、センタがプロバイダとして認めているエンティティに関する情報を保持したデータベースである。

【０１９２】

プロバイダＤＢ２０５の構造を図６に示す。プロバイダＤＢ２０５は以下の唯一の属性からなるテーブルである。

【０１９３】

【表１４】

プロバイダ識別子属性：センタがプロバイダとして認めているエンティティの識別子。

【０１９４】

センタは、このデータベースに登録されているプロバイダ以外のエンティティをプロバイダとは認めない。したがって、そのようなエンティティに対して検証用公開鍵情報を発行することはないし、そのようなエンティティが提供している物品やサービスに対する予約証明証を発行する事もない。

【０１９５】

センタがプロバイダと認めるエンティティを増やしたい場合には、このデータベースに新規エントリを追加する。

【０１９６】

公開鍵ペアＤＢ２０６は、プロバイダに発行される検証用公開鍵と、それに対応する秘密鍵に関する情報を保持したデータベースである。本実施例では、検証用公開鍵とそれに対応する秘密鍵のための公開鍵暗号アルゴリズムとしてＲＳＡを使用する。したがって、公開鍵ペアＤＢ２０６はＲＳＡの公開鍵ペアについての情報を保持するデータベースである。

【０１９７】

公開鍵ペアＤＢ２０６の構造を図７に示す。公開鍵ペアＤＢ２０６は以下の７つの属性からなるテーブルであり、各エントリはそれぞれ一つの公開鍵ペアに関する情報である。

【０１９８】

【表１５】

公開鍵識別子属性：このエントリの公開鍵ペアに割り当てられた検証用公開鍵識別子。

法数属性：ＲＳＡ法数。

公開鍵属性：ＲＳＡ公開鍵。

秘密鍵属性：ＲＳＡ秘密鍵。

プロバイダ識別子属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵

情報を発行されたプロバイダの識別子。

有効期間開始属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の有効期間の開始日時。

有効期間終了属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の有効期間の終了日時。

発行日属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の発行日時。

【０１９９】

リテーラＤＢ２０７は、センタがリテーラとして認めているエンティティに関する情報を保持したデータベースである。

【０２００】

リテーラＤＢ２０７の構造を図８に示す。リテーラＤＢ２０７は以下の唯一の属性からなるテーブルである。

【０２０１】

【表１６】

リテーラ識別子属性：センタがリテーラとして認めているエンティティの識別子。

【０２０２】

センタは、このデータベースに登録されているリテーラ以外のエンティティをリテーラとは認めない。したがって、そのようなエンティティからの予約証明証発行依頼に対して予約証明証を発行する事はない。

【０２０３】

センタがリテーラと認めるエンティティを増やしたい場合には、このデータベースに新規エントリを追加する。

【０２０４】

消費者ＤＢ２０８は、センタが消費者として認めているエンティティに関する情報を保持したデータベースである。

【０２０５】

消費者ＤＢ２０８の構造を図９に示す。消費者ＤＢ２０８は以下の２つの属性

からなるテーブルである。

【０２０６】

【表１７】

消費者識別子属性：センタが消費者として認めているエンティティの識別子。消費者が所持する携帯型記憶装置の中にも保持されている値である。

消費者秘密情報属性：消費者識別子属性で指定された消費者識別子を保持している携帯型記憶装置内に保持されている消費者秘密情報。

【０２０７】

予約証明証発行履歴ＤＢ２０９は、センタがこれまでに発行した予約証明証に関する情報を保持したデータベースである。

【０２０８】

予約証明証発行履歴ＤＢ２０９の構造を図１０に示す。予約証明証発行履歴ＤＢ２０９は以下の６つの属性からなるテーブルであり、各エントリはそれぞれ一つの予約証明証に関する情報である。

【０２０９】

【表１８】

公開鍵識別子属性：このエントリの予約証明証を検証できる検証用公開鍵に割り当てられた検証用公開鍵識別子。

プロバイダ識別子属性：このエントリの公開鍵識別子属性で指定された検証用公開鍵を含む検証用公開鍵情報の発行を受けたプロバイダの識別子。

消費者識別子属性：このエントリの予約証明証で予約を証された消費者が持つ携帯型記憶装置に含まれる消費者識別子。

仲介者識別子属性：このエントリの予約証明証の発行を依頼したリテーラの識別子。

予約条件属性：このエントリの予約証明証に記載された予約条件をＢＥＲ（Ｂａｓｉｃ　Ｅｎｃｏｄｉｎｇ　Ｒｕｌｅ：ＩＴＵ－Ｔ　Ｒｅｃｏｍｍｅｎｄａｔｉｏｎ　Ｘ．６９０）にしたがってエンコードした結果。

発行日属性：このエントリの予約証明証の発行日時。

【０２１０】

図３は、本実施例のセンタの動作を示すフローチャートである。本実施例のセンタの動作を図３のフローチャートにしたがって説明する。

【０２１１】

図３に示す通り、本実施例のセンタは、データの入力を待ち続け、入力があれば入力に応じた処理を行った後に再度入力待ちの状態に戻る終わる事のない処理である。

【０２１２】

最初に、入出力制御部２０１で入力があるかどうかがチェックされる（３０１）。ここで入力がなければ、再度入力のチェック（３０１）に戻る。

【０２１３】

入力のチェック（３０１）で入力があった場合、処理選択部２０２で、その入力が検証用公開鍵情報依頼かどうかが判断される（３０２）。入力が検証用公開鍵情報依頼であれば、検証用公開鍵情報依頼処理部２０３が呼び出され検証用公開鍵情報依頼が処理される（３０３）。検証用公開鍵情報依頼の処理が終われば、再度入力のチェック（３０１）に戻る。

【０２１４】

３０２の判断で、入力が検証用公開鍵情報依頼でなければ、処理選択部２０２で、その入力が予約証明証依頼どうかが判断される（３０４）。入力が予約証明証依頼であれば、予約証明証依頼処理部２０４が呼び出され予約証明証依頼が処理される（３０５）。予約証明証依頼の処理が終われば、再度入力のチェック（３０１）に戻る。

【０２１５】

また、３０４の判断で、入力が予約証明証依頼でなければ、再度入力のチェック（３０１）に戻る。

【０２１６】

［検証用公開情報依頼処理部］

図４は、本実施例のセンタが持つ検証用公開情報依頼処理部２０３の内部構成を示した図である。

【０２１７】

検証用公開情報依頼処理部２０３は、検証用公開情報依頼を処理する機能を持ち、処理制御部４０１、署名検証部４０２、公開鍵ペア作成部４０３、公開鍵ペア識別子作成部４０４、検証用公開鍵情報作成部４０５、検証用公開鍵情報送付作成部４０６、エラーメッセージ作成部４０７、署名作成部４０８から構成される。

【０２１８】

検証用公開情報依頼処理部２０３を構成する各部の役割を以下に述べる。

【０２１９】

処理制御部４０１：処理選択部２０２からの入力、入出力制御部２０１への出力、プロバイダＤＢ２０５の参照、公開鍵ペアＤＢ２０６へのエントリの追加の機能を担うとともに、検証用公開情報依頼の処理全体を制御する。

署名検証部４０２：処理選択部２０２から入力される検証用公開情報依頼のデジタル署名を検証する。

公開鍵ペア作成部４０３：検証用公開鍵および予約証明証の作成に使用される公開鍵ペアを作成する。

公開鍵ペア識別子作成部４０４：検証用公開鍵に割り当てられる検証用公開鍵識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

検証用公開鍵情報作成部４０５：検証用公開鍵情報を作成する。検証用公開鍵情報にデジタル署名を添付するために署名作成部４０８を呼び出す。

検証用公開鍵情報送付作成部４０６：検証用公開鍵情報送付を作成する。検証用公開鍵情報送付にデジタル署名を添付するために署名作成部４０８を呼び出す。さらに、センタの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部２１１にアクセスする。

エラーメッセージ作成部４０７：エラーメッセージを作成する。

署名作成部４０８：検証用公開鍵情報、検証用公開鍵情報送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部２１０にアクセスする。

【０２２０】

図５は、本実施例のセンタが持つ検証用公開情報依頼処理部２０３の処理制御部４０１の動作を示すフローチャートである。処理制御部４０１の動作を図５にしたがって説明する。

【０２２１】

まず、処理選択部２０２から入力された検証用公開情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子を取り出し、センタがこの識別子のエンティティをプロバイダとして認めているかどうかをプロバイダＤＢ２０５を参照して調べる（５０１）。プロバイダＤＢ２０５にこの識別子を持つエントリが存在すれば、プロバイダとして認めたエンティティであることがわかる。

【０２２２】

５０１の判断で、プロバイダとして認めていないエンティティであることがわかった場合、エラーメッセージ作成部４０７でエラーメッセージを作成して入出力制御部２０１に出力した後（５０９）、終了する。

【０２２３】

５０１の判断で、プロバイダとして認めているエンティティであることがわかった場合、検証用公開情報依頼のデジタル署名を検証する（５０２）。検証鍵は検証用公開情報依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１１１から公開鍵証明証を取得してから署名の検証を行う。

【０２２４】

署名の検証に失敗した場合、エラーメッセージ作成部４０７でエラーメッセージを作成して入出力制御部２０１に出力した後（５０９）、終了する。

【０２２５】

署名の検証に成功した場合、公開鍵ペア作成部４０３を呼び出してＲＳＡ公開鍵ペアを作成させ、作成された法数、公開鍵、秘密鍵を受け取る（５０３）。さらに、公開鍵ペア識別子作成部４０４を呼び出して検証用公開鍵情報に割り当てる識別子を作成させ、作成された識別子を受け取る（５０４）。

【０２２６】

次に検証用公開鍵情報の有効期間の開始日時と終了日時を適切に決定した後（５０５）、新しいエントリを公開鍵ペアＤＢに追加する（５０６）。新しいエントリの各属性には以下の値が設定される。

【０２２７】

【表１９】

公開鍵識別子属性：５０４で作成した識別子。

法数属性：５０３で作成したＲＳＡ法数。

公開鍵属性：５０３で作成したＲＳＡ公開鍵。

秘密鍵属性：５０３で作成したＲＳＡ秘密鍵。

プロバイダ識別子属性：検証用公開情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子。

有効期間開始属性：５０５で作成した有効期間の開始日時。

有効期間終了属性：５０５で作成した有効期間の終了日時。

発行日属性：現在の日時。

【０２２８】

次に、検証用公開鍵情報作成部（４０５）を呼び出し、検証用公開鍵情報を作成させ、その結果を受け取る（５０７）。検証用公開鍵情報の各フィールドには以下の値が設定される。

【０２２９】

【表２０】

発行者フィールド：自分自身すなわちセンタの識別子。

受領者フィールド：検証用公開情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子。

発行日フィールド：現在の時刻。

有効期間開始日時フィールド：５０５で作成した有効期間の開始日時。

有効期間終了日時フィールド：５０５で作成した有効期間の終了日時。

検証用公開鍵鍵識別子フィールド：５０４で作成した識別子。

公開鍵情報フィールド：５０３で作成した法数、公開鍵、秘密鍵。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデ

ジタル署名。デジタル署名の作成のため、署名作成部４０８を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

【０２３０】

最後に、検証用公開鍵情報送付作成部４０６を呼び出し、検証用公開鍵情報送付を作成させ、その結果を受け取って入出力制御部２０１に出力した後（５０８）、終了する。検証用公開鍵情報送付の各フィールドには以下の値が設定される。

【０２３１】

【表２１】

発信者フィールド：自分自身すなわちセンタの識別子。

受信者フィールド：検証用公開情報依頼の発信者フィールドに記載されている識別子。

日時フィールド：現在の時刻。

検証用公開鍵情報フィールド：５０７で作成した検証用公開鍵情報。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部４０８を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部２１１に記憶している公開鍵証明証。

【０２３２】

［予約証明証依頼処理部］

図１１は、本実施例のセンタが持つ予約証明証依頼処理部２０４の内部構成を示した図である。

【０２３３】

予約証明証依頼処理部２０４は、予約証明証依頼を処理する機能を持ち、処理制御部１１０１、署名検証部１１０２、予約証明証仲介許諾内容確認部１１０３、予約証明証識別子作成部１１０４、予約証明証作成部１１０５、予約証明証送付作成部１１０６、エラーメッセージ作成部１１０７、署名作成部１１０８、予約値作成部１１０９、予約条件作成部１１１０から構成される。

【０２３４】

予約証明証依頼処理部２０４を構成する各部の役割を以下に述べる。

【０２３５】

処理制御部１１０１：処理選択部２０２からの入力、入出力制御部２０１への出力、公開鍵ペアＤＢ２０６リテーラＤＢ２０７消費者ＤＢ２０８の参照、予約証明証発行履歴ＤＢ２０９へのエントリの追加の機能を担うとともに、予約証明証依頼の処理全体を制御する。

署名検証部１１０２：処理選択部２０２から入力される予約証明証依頼、および該予約証明証依頼に含まれる予約証明証仲介許諾のデジタル署名を検証する。

予約証明証仲介許諾内容確認部１１０３：処理選択部２０２から入力される予約証明証依頼で依頼された予約証明証の仲介が、該予約証明証依頼に含まれている予約証明証仲介許諾によって許諾されているかどうかを確認する。

予約証明証識別子作成部１１０４：予約証明証に割り当てられる予約証明証識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

予約証明証作成部１１０５：予約証明証を作成する。予約証明証にデジタル署名を添付するために署名作成部１１０８を呼び出す。

予約証明証送付作成部１１０６：予約証明証送付を作成する。予約証明証送付にデジタル署名を添付するために署名作成部１１０８を呼び出す。さらに、センタの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部２１１にアクセスする。

エラーメッセージ作成部１１０７：エラーメッセージを作成する。

署名作成部１１０８：予約証明証、予約証明証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部２１０にアクセスする。

予約値作成部１１０９：予約証明証に含まれる予約値を作成する。

予約条件作成部１１１０：予約証明証に含まれる予約条件を作成する。

【０２３６】

図１２は、本実施例のセンタが持つ予約証明証依頼処理部２０４の処理制御部１１０１の動作を示すフローチャートである。処理制御部１１０１の動作を図１

２にしたがって説明する。

【０２３７】

まず、処理選択部２０２から入力された予約証明証依頼の発信者フィールドに記載されている識別子を取り出し、センタがこの識別子のエンティティをリテーラとして認めているかどうかをリテーラＤＢ２０７を参照して調べる（１２０１）。リテーラＤＢ２０７にこの識別子を持つエントリが存在すれば、リテーラとして認めたエンティティであることがわかる。

【０２３８】

１２０１の判断で、リテーラとして認めていないエンティティであることがわかった場合、エラーメッセージ作成部１１０７でエラーメッセージを作成して入出力制御部２０１に出力した後（１２１０）、終了する。

【０２３９】

１２０１の判断で、リテーラとして認めているエンティティであることがわかった場合、予約証明証依頼のデジタル署名、および予約証明証依頼に含まれる予約証明証仲介許諾のデジタル署名を検証する（１２０２）。検証鍵は予約証明証依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１１１から公開鍵証明証を取得してから署名の検証を行う。

【０２４０】

署名の検証に失敗した場合、エラーメッセージ作成部１１０７でエラーメッセージを作成して入出力制御部２０１に出力した後（１２１０）、終了する。

【０２４１】

署名の検証に成功した場合、予約証明証依頼で依頼された予約証明証の仲介が、該予約証明証依頼に含まれている予約証明証仲介許諾によって許諾されているかどうかを確認する（１２０３）。より具体的には、予約証明証依頼の予約内容フィールドに含まれている予約仕様を予約証明証仲介許諾内容確認部１１０３に送付し、該予約仕様の公開鍵鍵識別子フィールドで指定されている検証用公開鍵識別子を持つ検証用公開鍵に対応する予約証明証を、該予約仕様の予約条件フィールドに記載されている予約条件で発行することが、該予約仕様の予約証明証仲

介許諾フィールドに含まれている予約証明証仲介許諾で許諾されているかどうかを確認する。

【０２４２】

１２０３で、許諾されていない事がわかった場合、エラーメッセージ作成部１１０７でエラーメッセージを作成して入出力制御部２０１に出力した後（１２１０）、終了する。

【０２４３】

１２０３で、許諾されている事がわかった場合、予約証明証識別子作成部１１０４を呼び出して予約証明証に割り当てる識別子を作成させ、作成された識別子を受け取った後（１２０４）、予約条件作成部１１１０を呼び出して、予約証明証に記載する予約条件を決定する（１２０５）。予約条件作成部が生成する予約条件は、予約証明証依頼予約内容フィールドに含まれている予約仕様の予約条件フィールドの値そのままでもよいし、該予約仕様の予約証明証仲介許諾フィールドに含まれている予約証明証仲介許諾によって許諾されている範囲内で該予約条件フィールドの値を適切に修正してもよい。

【０２４４】

予約条件の作成の後、新しいエントリを予約証明証発行履歴ＤＢ２０９に追加する（１２０６）。新しいエントリの各属性には以下の値が設定される。

【０２４５】

【表２２】

公開鍵識別子属性：予約証明証依頼の予約内容フィールドに含まれている予約仕様の公開鍵鍵識別子フィールドの値。

プロバイダ識別子属性：公開鍵ペアＤＢにアクセスし、該公開鍵ペアＤＢの公開鍵識別子属性が、予約証明証依頼の予約内容フィールドに含まれている予約仕様の公開鍵鍵識別子フィールドの値と同じ値を持つエントリの、プロバイダ識別子属性を取り出し、その値を設定する。

消費者識別子属性：予約証明証依頼の予約内容フィールドに含まれている予約仕様の消費者識別子フィールドの値。

仲介者識別子属性：予約証明証依頼の発信者フィールドの値。

予約条件属性：１２０５で予約条件作成部が作成した予約条件。

発行日属性：現在の日時。

【０２４６】

次に、予約値作成部１１０９を呼び出して予約値を作成させ、その結果を受け取る（１２０７）。

【０２４７】

次に、予約証明証作成部１１０５を呼び出し、予約証明証を作成させ、その結果を受け取る（１２０８）。予約証明証の各フィールドには以下の値が設定される。

【０２４８】

【表２３】

発行者フィールド：自分自身すなわちセンタの識別子。

受領者フィールド：　予約証明証依頼の予約内容フィールドに含まれている予約仕様の消費者識別子フィールドの値。

発行日フィールド：１２０６で予約証明証発行履歴ＤＢ２０９に追加したエントリの発行日属性の値。

予約証明証識別子フィールド：１２０４で作成した識別子。

公開鍵識別子フィールド：予約証明証依頼の予約内容フィールドに含まれている予約仕様の公開鍵鍵識別子フィールドの値。

予約条件フィールド：１２０５で予約条件作成部が作成した予約条件。

予約値フィールド：１２０７で作成した予約値。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部１１０８を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

【０２４９】

最後に、予約証明証送付作成部１１０６を呼び出し、予約証明証送付を作成させ、その結果を受け取って入出力制御部２０１に出力した後（１２０９）、終了する。予約証明証送付の各フィールドには以下の値が設定される。

【０２５０】

【表２４】

発信者フィールド：自分自身すなわちセンタの識別子。

受信者フィールド：予約証明証依頼の発信者フィールドの値。

日時フィールド：現在の時刻。

予約証明証フィールド：１２０８で作成した予約証明証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部１１０８を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部２１１に記憶している公開鍵証明証。

【０２５１】

[センタが持つその他の機能]

本実施例のセンタは、予約証明証発行の履歴情報をプロバイダに送付する事ができる。

【０２５２】

プロバイダに渡される予約証明証発行の履歴情報は、そのプロバイダに割り当てられた検証用公開鍵に対応する予約証明証の発行についての情報であり、予約証明証発行プロバイダ用履歴作成部２１２で作成され、入出力制御部２０１を介してプロバイダに送付される。プロバイダにとっては、この履歴情報は、自己が提供している物品やサービスをどのリテーラがどのぐらい予約販売したかのを示す信頼できる情報であり、予約販売におけるマージンがリテーラからプロバイダに渡される場合に、リテーラから送られたマージンの正しさをプロバイダが確認する際の重要な情報となる。

【０２５３】

予約証明証発行プロバイダ用履歴作成部２１２は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証発行履歴ＤＢ２０９から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その公開鍵識別子属性、仲介者識別子属性、予約条件属性、発行日属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子

と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【０２５４】

本実施例のセンタは、予約証明証発行の履歴情報をリテーラにも送付する事ができる。

【０２５５】

リテーラに渡される予約証明証発行の履歴情報は、そのリテーラからの依頼で行った予約証明証の発行についての情報であり、予約証明証発行リテーラ用履歴作成部２１３で作成され、入出力制御部２０１を介してリテーラに送付される。この履歴は、センタがリテーラから予約証明証発行のマージンを受け取る場合のマージンの額の根拠となる。

【０２５６】

予約証明証発行リテーラ履歴作成部２１３は、履歴を作成するリテーラの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証発行履歴ＤＢ２０９から、仲介者識別子属性の値が指定されたリテーラの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その公開鍵識別子属性、プロバイダ識別子属性、消費者識別子属性、予約条件属性、発行日属性の値を取り出す。本実施例では、履歴を作成するリテーラの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でリテーラから入力されるように構成してもよい。

【０２５７】

また、本実施例のセンタは、検証用公開鍵情報発行の履歴情報をプロバイダに送付する事ができる。

【０２５８】

プロバイダに渡される検証用公開鍵情報発行の履歴情報は、そのプロバイダに対して発行された検証用公開鍵情報についての情報であり、検証用公開鍵情報発行履歴作成部２１４で作成され、入出力制御部２０１を介してプロバイダに送付される。この履歴は、センタがプロバイダから検証用公開鍵情報発行の手数料を徴収する場合の根拠となる。

【０２５９】

検証用公開鍵情報発行履歴作成部２１４は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、公開鍵ペアＤＢ２０６から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発効日属性の値が指定された履歴作成の対象期間内であるエントリ郡を取り出し、その公開鍵識別子属性、法数属性、公開鍵属性、有効期間開始属性、有効期間終了属性、発行日属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【０２６０】

上記の履歴情報のプロバイダやリテーラへの送付方法は、電子メールでもよいし、ＷＷＷベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

【０２６１】

［プロバイダの構成］

図１３は、本実施例のプロバイダの構成図である。

【０２６２】

本実施例のプロバイダは、検証用公開鍵情報依頼を作成してインターネットを介してセンタに送付する機能と、インターネットを介して入力される検証用公開鍵情報送付と予約証明証仲介許諾依頼とを処理する機能を持つ。プロバイダは、入出力制御部１３０１、処理選択部１３０２、検証用公開鍵情報依頼作成部１３０３、検証用公開鍵情報送付処理部１３０４、予約証明証仲介許諾依頼処理部１３０５、検証用公開鍵ＤＢ１３０６、署名鍵記憶部１３０７、証明証記憶部１３０８、予約証明証仲介許諾発行履歴ＤＢ１３０９、予約証明証仲介許諾発行履歴作成部１３１０から構成され、入出力制御部１３０１を介してインターネットに接続されている。

【０２６３】

本実施例のプロバイダの各部の役割を以下に述べる。

【０２６４】

入出力制御部１３０１：インターネットを介したデータの入力を監視するとともに、検証用公開鍵情報依頼作成部１３０３や予約証明証仲介許諾依頼処理部１３０５が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部１３０１への入力、あるいは、入出力制御部１３０１からインターネットへの出力の方法としては、入出力制御部１３０１と接続されたWWWサイトを準備して他のエンティティにアクセスさせるもの、他のエンティティが用意しているWWWサイトにアクセスしてプロバイダが作成したデータを送るもの、あるいは電子メールシステムと入出力制御部１３０１を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部１３０２：入力したデータが検証用公開鍵情報送付かまたは予約証明証仲介許諾依頼かを判断し、検証用公開鍵情報送付であれば検証用公開鍵情報送付処理部１３０４を、予約証明証仲介許諾依頼であれば予約証明証仲介許諾依頼処理部１３０５を呼び出す。

検証用公開鍵情報依頼作成部１３０３：検証用公開鍵情報依頼を作成し、入出力制御部１３０１を介してセンタに送付する。検証用公開鍵情報依頼作成の過程で、署名鍵記憶部１３０７と証明証記憶部１３０８にアクセスする。

検証用公開鍵情報送付処理部１３０４：検証用公開鍵情報送付を処理し、検証用公開鍵を検証用公開鍵ＤＢ１３０６に登録する。

予約証明証仲介許諾依頼処理部１３０５：予約証明証仲介許諾依頼を処理し、予約証明証仲介許諾送付を作成して入出力制御部１３０１を介して依頼者に送付する。予約証明証仲介許諾送付作成の過程で検証用公開鍵ＤＢ１３０６を参照し、予約証明証仲介許諾ＤＢに新しいエントリを追加するとともに、署名鍵記憶部１３０７と証明証記憶部１３０８にアクセスする。

検証用公開鍵ＤＢ１３０６：検証用公開鍵に関する情報を保持するＤＢ。

署名鍵記憶部１３０７：プロバイダが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部１３０８：署名鍵記憶部１３０７に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

予約証明証仲介許諾発行履歴ＤＢ１３０９：予約証明証仲介許諾の発行の履歴を

保持するＤＢ。

予約証明証仲介許諾発行履歴作成部１３１０：リテーラ毎の予約証明証仲介許諾の発行履歴を作成する。

【０２６５】

［プロバイダが持つデータベース］

プロバイダは、検証用公開鍵ＤＢ１３０６、予約証明証仲介許諾発行履歴ＤＢ１３０９の２つのデータベースを持っている。

【０２６６】

検証用公開鍵ＤＢ１３０６は、センタから発行を受けた検証用公開鍵情報の内容を、プロバイダ自身が決定した検証用公開鍵の用途とともに保持するデータベースである。

【０２６７】

検証用公開鍵ＤＢ１３０６の構造を図１４に示す。検証用公開鍵ＤＢ１３０６は以下の６つの属性からなるテーブルであり、各エントリはそれぞれ一つの検証用公開鍵に関する情報である。

【０２６８】

【表２５】

公開鍵識別子属性：検証用公開鍵に割り当てられた検証用公開鍵識別子。

法数属性：検証用公開鍵情報に含まれていたＲＳＡ法数。

公開鍵属性：検証用公開鍵情報に含まれていたＲＳＡ公開鍵。

有効期間開始属性：検証用公開鍵情報の有効期間の開始日時。

有効期間終了属性：検証用公開鍵情報の有効期間の終了日時。

用途属性：このエントリの検証用公開鍵に対してプロバイダが割り当てた用途。この検証用公開鍵で予約証明証の正当性を検証する物品やサービスの情報である。

【０２６９】

予約証明証仲介許諾発行履歴ＤＢ１３０９は、プロバイダが発行した予約証明証仲介許諾に関する履歴を保持するデータベースである。

【０２７０】

予約証明証仲介許諾発行履歴ＤＢ１３０９の構造を図３４に示す。予約証明証仲介許諾発行履歴ＤＢ１３０９は以下の７つの属性からなるテーブルであり、各エントリはそれぞれ一回の予約証明証仲介許諾の発行に関する情報である。

【０２７１】

【表２６】

予約証明証仲介許諾識別子属性：発行した予約証明証仲介許諾に割り当てられた識別子。

公開鍵識別子属性：発行した予約証明証仲介許諾で予約証明証の仲介が許諾される検証用公開鍵に割り当てられた検証用公開鍵識別子。

リテーラ識別子属性：発行した予約証明証仲介許諾で許諾をうけるリテーラの識別子。

予約条件限定情報属性：発行した予約証明証仲介許諾に記載されている予約条件限定情報。

有効期間開始属性：発行した予約証明証仲介許諾の有効期間の開始日時。

有効期間終了属性：発行した予約証明証仲介許諾の有効期間の終了日時。

発行日属性：発行した予約証明証仲介許諾の発行日時。

【０２７２】

［検証用公開鍵情報依頼作成部］

本実施例のプロバイダは、新たに予約販売を開始したい物品やサービスが発生した時に、その物品やサービスに割り当てる検証用公開鍵を含む検証用公開鍵情報の発行をセンタに依頼する。依頼の際には、検証用公開鍵情報依頼作成部１３０３において検証用公開鍵情報依頼を作成し、入出力制御部１３０１を介してセンタに送付する。

【０２７３】

検証用公開鍵情報依頼作成部１３０３では、検証用公開鍵情報依頼の各フィールドに以下の値を設定する。

【０２７４】

【表２７】

発信者フィールド：自分自身すなわちプロバイダの識別子。

受信者フィールド：センタの識別子。

日時フィールド：現在の時刻。

公開鍵仕様フィールド：作成してもらう検証用公開鍵に対する要望。検証用公開鍵の使用者として自分の識別子を記載し、さらに、要望する公開鍵暗号アルゴリズムと鍵長が記載される。本実施例では公開鍵暗号アルゴリズムとしてはＲＳＡのみが仕様可能なので、公開鍵暗号アルゴリズムの値はＲＳＡで固定である。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、検証用公開鍵情報依頼作成部１３０３は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部１３０７にアクセスして入手する。

【０２７５】

【表２８】

証明証フィールド：証明証記憶部１３０８に記憶している公開鍵証明証。

【０２７６】

［検証用公開鍵情報送付処理部］

検証用公開鍵情報依頼作成部１３０３で検証用公開鍵情報依頼が作成されセンタに送付されると、その返信としてセンタから検証用公開鍵情報送付が送信されてくる。検証用公開鍵情報送付は、入出力制御部１３０１および処理選択部１３０２を経由して検証用公開鍵情報送付処理部１３０４に送られ、そこで処理される。

【０２７７】

図１５は、本実施例のプロバイダが持つ検証用公開情報送付処理部１３０４の動作を示すフローチャートである。検証用公開情報送付処理部１３０４の動作を図１５にしたがって説明する。

【０２７８】

まず、処理選択部１３０２から入力された検証用公開情報送付、および、該検証用公開情報送付に含まれる検証用公開鍵情報のデジタル署名を検証する（１５０１）。検証鍵は検証用公開情報送付の証明証フィールドに添付されているもの

を使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１１１から公開鍵証明証を取得してから署名の検証を行う。署名の検証のために、検証用公開情報送付処理部１３０４はデジタル署名の検証を専門に行う署名検証部を含んでいる。

【０２７９】

１５０１で、デジタル署名の検証に失敗した場合、エラー処理を行った後（１５０５）、終了する。

【０２８０】

１５０１で、デジタル署名の検証に成功した場合、検証用公開情報送付に含まれている検証用公開鍵情報の発行者がセンタであるかどうかが調べられる（１５０２）。この検査は、検証用公開鍵情報の発行者フィールドに記載されている識別子がセンタのものであるかどうかで検査できる。

【０２８１】

１５０２の検査で、検証用公開鍵情報の発行者がセンタでなかった場合、エラー処理を行った後（１５０５）、終了する。

【０２８２】

１５０２の検査で、検証用公開鍵情報の発行者がセンタであったら、次に検証用公開鍵ＤＢ１３０６に新しいエントリを追加する（１５０３）。新しいエントリの各属性には以下の値が設定される。

【０２８３】

【表２９】

公開鍵識別子属性：検証用公開情報送付に含まれている検証用公開鍵情報の検証用公開鍵識別子フィールドの値。

法数属性：検証用公開情報送付に含まれている検証用公開鍵情報の、公開鍵情報フィールドに含まれていたＲＳＡ法数。

公開鍵属性：検証用公開情報送付に含まれている検証用公開鍵情報の、公開鍵情報フィールドに含まれていたＲＳＡ公開鍵。

有効期間開始属性：検証用公開情報送付に含まれている検証用公開鍵情報の有効期間開始日時フィールドの値。

有効期間終了属性：検証用公開情報送付に含まれている検証用公開鍵情報の有効期間終了日時フィールドの値。

用途属性：この検証用公開鍵にプロバイダが割り当てた用途についての情報。

【０２８４】

［予約証明証仲介許諾依頼処理部］

図１６は、本実施例のプロバイダが持つ予約証明証仲介許諾依頼処理部１３０５の内部構成を示した図である。

【０２８５】

予約証明証仲介許諾依頼処理部１３０５は、予約証明証仲介許諾依頼を処理する機能を持ち、処理制御部１６０１、署名検証部１６０２、予約証明証仲介許諾識別子作成部１６０３、エラーメッセージ作成部１６０４、予約証明証仲介許諾作成部１６０５、予約証明証仲介許諾送付作成部１６０６、署名作成部１６０７、予約条件限定情報作成部１６０８から構成される。

【０２８６】

予約証明証仲介許諾依頼処理部１３０５を構成する各部の役割を以下に述べる。

【０２８７】

処理制御部１６０１：処理選択部１３０２からの入力、入出力制御部１３０１への出力、検証用公開鍵ＤＢ１３０６の参照、予約証明証仲介許諾発行履歴ＤＢ１３０９へのエントリの追加の機能を担うとともに、予約証明証仲介許諾依頼の処理全体を制御する。

署名検証部１６０２：処理選択部２０２から入力される予約証明証仲介許諾依頼のデジタル署名を検証する。

予約証明証仲介許諾識別子作成部１６０３：予約証明証仲介許諾に割り当てられる予約証明証仲介許諾識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

エラーメッセージ作成部１６０４：エラーメッセージを作成する。

予約証明証仲介許諾作成部１６０５：予約証明証仲介許諾を作成する。予約証明証仲介許諾にデジタル署名を添付するために署名作成部１６０７を呼び出す。

予約証明証仲介許諾送付作成部１６０６：予約証明証仲介許諾送付を作成する。予約証明証仲介許諾送付にデジタル署名を添付するために署名作成部１６０７を呼び出す。さらに、プロバイダの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部１３０８にアクセスする。

署名作成部１６０７：予約証明証仲介許諾、予約証明証仲介許諾送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部１３０７にアクセスする。

予約条件限定情報作成部１６０８：予約証明証仲介許諾に記載される予約条件限定情報を作成する。

【０２８８】

図１７は、本実施例のプロバイダが持つ予約証明証仲介許諾依頼処理部１３０５の処理制御部１６０１の動作を示すフローチャートである。処理制御部１６０１の動作を図１７にしたがって説明する。

【０２８９】

まず、処理選択部１３０２から入力された予約証明証仲介許諾依頼のデジタル署名を検証する（１７０１）。検証鍵は予約証明証仲介許諾依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１１１から公開鍵証明証を取得してから署名の検証を行う。

【０２９０】

署名の検証に失敗した場合、エラーメッセージ作成部１６０４でエラーメッセージを作成して入出力制御部１３０１に出力した後（１７０９）、終了する。

【０２９１】

署名の検証に成功した場合、予約証明証仲介許諾依頼で依頼された予約証明証仲介許諾を発行するかどうかを決定する（１７０２）。予約証明証仲介許諾を発行するかどうかの決定はプロバイダにまかされている。例えば、予約証明証仲介許諾によって許諾を受けるリテーラを信用できない場合や、予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の許諾者フィールドに記載されている識別子が自分のものと異なる場合や、予約証明証仲介許諾依頼に含まれる予約証明

証仲介許諾仕様の公開鍵鍵識別子フィールドに記載された検証用公開鍵識別子を持つ検証用公開鍵情報が自分に対して発行されたものでない場合や、予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の希望予約条件限定情報フィールドの希望にそえない場合に予約証明証仲介許諾の発行をやめることになる。

【０２９２】

１７０２で、予約証明証仲介許諾を発行しないと決定した場合には、エラーメッセージ作成部１６０４でエラーメッセージを作成して入出力制御部１３０１に出力した後（１７０９）、終了する。

【０２９３】

１７０２で、予約証明証仲介許諾を発行すると決定した場合には、予約証明証仲介許諾識別子作成部１６０３を呼び出して予約証明証仲介許諾に割り当てる識別子を作成させ、作成された識別子を受け取った後（１７０３）、発行する予約証明証仲介許諾の有効期間を適切に決定する（１７０４）。

【０２９４】

さらに、予約条件限定情報作成部１６０８を呼び出して発行する予約証明証仲介許諾に含まれる予約条件限定情報を作成させ、その結果を受け取る（１７０５）。ここで作成する予約条件限定情報は、予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の希望予約条件限定情報フィールドに記載されいるものでもよいし、プロバイダが自己の判断で適切な予約条件限定情報を決定してもよい。

【０２９５】

次に、予約証明証仲介許諾作成部１６０５を呼び出し、予約証明証仲介許諾を作成させ、その結果を受け取る（１７０６）。予約証明証仲介許諾の各フィールドには以下の値が設定される。

【０２９６】

【表３０】

発行者フィールド：自分自身すなわちプロバイダの識別子。

受領者フィールド：予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の被許諾者フィールドの値。

発行日フィールド：現在の日時。

予約証明証仲介許諾識別子フィールド：１７０３で作成した識別子。

有効期間開始日時フィールド：１７０４で決定した有効期間の開始日時。

有効期間終了日時フィールド：１７０４で決定した有効期間の終了日時。

公開鍵鍵識別子フィールド：予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の公開鍵鍵識別子フィールドの値。

予約条件限定情報フィールド：１７０５で決定した予約条件限定情報の値。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部１６０７を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

【０２９７】

次に、予約証明証仲介許諾送付作成部１６０６を呼び出し、予約証明証仲介許諾送付を作成させ、その結果を受け取って入出力制御部１３０１に出力する（１７０７）。予約証明証仲介許諾送付の各フィールドには以下の値が設定される。

【０２９８】

【表３１】

発信者フィールド：自分自身すなわちプロバイダの識別子。

受信者フィールド：予約証明証仲介許諾依頼の発信者フィールドに記載されている識別子。

日時フィールド：現在の日時。

予約証明証仲介許諾フィールド：１７０６で作成した予約証明証仲介許諾。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部１６０７を呼び出し、結果の署名値をこのフィールドに設定する。

証明証フィールド：証明証記憶部１３０８に記憶している公開鍵証明証。

【０２９９】

最後に予約証明証仲介許諾発行の履歴を表す新しいエントリを予約証明証仲介許諾発行履歴ＤＢ１３０９に追加して終了する。追加されるエントリの各属性には以下の値が格納される。

【０３００】

【表３２】

予約証明証仲介許諾識別子属性：１７０３で作成した識別子。

公開鍵識別子属性：予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の公開鍵識別子フィールドの値。

リテーラ識別子属性：予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の被許諾者フィールドの値。

予約条件限定情報属性：１７０５で決定した予約条件限定情報の値。

有効期間開始属性：１７０４で決定した有効期間の開始日時。

有効期間終了属性：１７０４で決定した有効期間の終了日時。

発行日属性：１７０６で作成した予約証明証仲介許諾の発行日フィールドに記載した値。

【０３０１】

［プロバイダが持つその他の機能］

本実施例のプロバイダは、予約証明証仲介許諾発行の履歴情報をリテーラに送付する事ができる。

【０３０２】

リテーラに渡される予約証明証仲介許諾発行の履歴情報は、そのリテーラに発行された予約証明証仲介許諾についての情報であり、予約証明証仲介許諾発行履歴作成部１３１０で作成され、入出力制御部１３０１を介してリテーラに送付される。この履歴は、プロバイダがリテーラに対して予約証明証仲介許諾発行の手数料を請求する場合の根拠となる。

【０３０３】

予約証明証仲介許諾発行履歴作成部１３１０は、履歴を作成するリテーラの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証仲介許諾発行履歴ＤＢ１３０９から、リテーラ識別子属性の値が指定されたリテーラの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その予約証明証仲介許諾識別子属性、公開鍵識別子属性、予約条件限定情報属性、有効期間開始属性、有効期間終了属性、発行日属性の値

を取り出す。本実施例では、履歴を作成するリテーラの識別子と履歴作成の対象期間の指定はプロバイダのオペレータから受けるが、インターネット経由でリテーラから入力されるように構成してもよい。

【０３０４】

上記の履歴情報の送付方法は、電子メールでもよいし、ＷＷＷベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

【０３０５】

［リテーラの構成］

図１８は、本実施例のリテーラの構成図である。

【０３０６】

本実施例のリテーラは、予約証明証仲介許諾依頼を作成してインターネットを介してプロバイダに送付する機能、インターネットを介して入力される予約証明証仲介許諾送付、予約証明証依頼、予約証明証送付を処理する機能、予約証明証仲介の履歴を作成してインターネットを介してプロバイダや予約証明証仲介の依頼者に送付する機能を持つ。リテーラは、入出力制御部１８０１、処理選択部１８０２、予約証明証仲介許諾依頼作成部１８０３、予約証明証依頼処理部１８０４、予約証明証仲介許諾送付処理部１８０５、予約証明証送付処理部１８０６、予約証明証仲介許諾ＤＢ１８０７、予約証明証仲介履歴ＤＢ１８０８、署名鍵記憶部１８０９、証明証記憶部１８１０、予約証明証仲介プロバイダ用履歴作成部１８１１、予約証明証仲介依頼者用履歴作成部１８１２から構成され、入出力制御部１８０１を介してインターネットに接続されている。

【０３０７】

本実施例のリテーラの各部の役割を以下に述べる。

【０３０８】

入出力制御部１８０１：インターネットを介したデータの入力を監視するとともに、予約証明証仲介許諾依頼作成部１８０３、予約証明証依頼処理部１８０４、予約証明証送付処理部１８０６が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部１８０４への入力、あるいは、入出力

制御部１８０４からインターネットへの出力の方法としては、入出力制御部１８０４と接続されたWWWサイトを準備して他のエンティティにアクセスさせるもの、他のエンティティが用意しているWWWサイトにアクセスしてリテーラが作成したデータを送るもの、あるいは電子メールシステムと入出力制御部１８０４を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部１８０２：入力したデータが、予約証明証依頼、予約証明証仲介許諾送付、予約証明証送付のいずれであるかを判断し、予約証明証依頼であれば予約証明証依頼処理部１８０４を、予約証明証仲介許諾送付であれば予約証明証仲介許諾送付処理部１８０５を、予約証明証送付であれば予約証明証送付処理部１８０６を呼び出す。

予約証明証仲介許諾依頼作成部１８０３：予約証明証仲介許諾依頼を作成し、入出力制御部１８０１を介してプロバイダに送付する。予約証明証仲介許諾依頼作成の過程で、署名鍵記憶部１８０９と証明証記憶部１８１０にアクセスする。

予約証明証依頼処理部１８０４：消費者からの予約証明証依頼を処理し、第二の予約証明証依頼を作成して、入出力制御部１８０１を介してセンタに送付する。処理の過程で、予約証明証仲介許諾ＤＢ１８０７を参照するとともに、予約証明証仲介履歴ＤＢ１８０８に新しいエントリを追加する。さらに、署名鍵記憶部１８０９と証明証記憶部１８１０にアクセスする。

予約証明証仲介許諾送付処理部１８０５：プロバイダからの予約証明証仲介許諾送付を処理し、該予約証明証仲介許諾送付に含まれている予約証明証仲介許諾を予約証明証仲介許諾ＤＢ１８０７に登録する。

予約証明証送付処理部１８０６：センタから送付された予約証明証送付を処理し、第二の予約証明証送付を作成して、入出力制御部１８０１を介して消費者に送付する。処理の過程で、予約証明証仲介履歴ＤＢ１８０８のエントリを更新するとともに、署名鍵記憶部１８０９と証明証記憶部１８１０にアクセスする。

予約証明証仲介許諾ＤＢ１８０７：プロバイダからこのリテーラに対して発行された予約証明証仲介許諾を保持するＤＢ。

予約証明証仲介履歴ＤＢ１８０８：このリテーラが仲介した予約証明証についての履歴を保持するＤＢ。

署名鍵記憶部１８０９：リテーラが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部１８１０：署名鍵記憶部１８０９に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

予約証明証仲介プロバイダ用履歴作成部１８１１：各プロバイダ毎の予約証明証仲介の履歴を作成し、入出力制御部１８０１を介してプロバイダに送付する。

予約証明証仲介依頼者用履歴作成部１８１２：リテーラが受け取った予約証明証仲介依頼の依頼者毎の予約証明証仲介の履歴を作成し、入出力制御部１８０１を介して依頼者に送付する。

【０３０９】

[リテーラが持つデータベース]

リテーラは、予約証明証仲介許諾ＤＢ１８０７と予約証明証仲介履歴ＤＢ１８０８の２つのデータベースを持っている。

【０３１０】

予約証明証仲介許諾ＤＢ１８０７は、リテーラが複数のプロバイダから受けた予約証明証仲介許諾に関する情報を保持したデータベースである。

【０３１１】

予約証明証仲介許諾ＤＢ１８０７の構造を図１９に示す。予約証明証仲介許諾ＤＢ１８０７は以下の５つの属性からなるテーブルである。各エントリがそれぞれ一つの予約証明証仲介許諾にあたる。

【０３１２】

【表３３】

予約証明証仲介許諾識別子属性：プロバイダから発行された予約証明証仲介許諾に割り当てられている予約証明証仲介許諾識別子。

公開鍵識別子属性：プロバイダから発行された予約証明証仲介許諾で予約証明証依頼の仲介が許諾された検証用公開鍵の識別子。

プロバイダ識別子属性：予約証明証仲介許諾を発行したプロバイダの識別子。

予約証明証仲介許諾属性：プロバイダから発行された予約証明証仲介許諾自体をＢＥＲにしたがってエンコードしたデータ。

プロバイダ証明証属性：予約証明証仲介許諾を発行したプロバイダのデジタル署名を検証できる公開鍵を含む公開鍵証明証をＢＥＲにしたがってエンコードしたデータ。

【０３１３】

予約証明証仲介履歴ＤＢ１８０８は、リテーラが仲介した予約証明証に関する情報を保持したデータベースである。

【０３１４】

予約証明証仲介履歴ＤＢ１８０８の構造を図２０に示す。予約証明証仲介履歴ＤＢ１８０８は以下の８つの属性からなるテーブルである。各エントリがそれぞれ一つの予約証明証の仲介にあたる。

【０３１５】

【表３４】

予約証明証識別子属性：仲介した予約証明証にセンタが割り当てた識別子。

公開鍵識別子属性：仲介した予約証明証の正当性を検証できる検証用公開鍵にセンタが割り当てた識別子。

プロバイダ識別子属性：公開鍵識別子属性で指定された検証用公開鍵情報のユーザであるプロバイダの識別子。

消費者識別子属性：予約証明証の発行を受けた消費者の識別子。

依頼者識別子属性：予約証明証依頼をリテーラに送付してきたエンティティの識別子。

予約条件属性：仲介された予約証明証に記載された予約条件。

依頼日時属性：リテーラが受け取った予約証明証依頼の作成日時。

発信日時属性：リテーラが予約証明証送付を作成した日時。

【０３１６】

［予約証明証仲介許諾依頼作成部］

本実施例のリテーラは、プロバイダが提供している物品やサービスの予約販売を始めたい場合、その物品やサービスに割りあてられた検証用公開鍵に対応する予約証明証の仲介を許諾する予約証明証仲介許諾をプロバイダから受けなければならない。プロバイダから予約証明証仲介許諾を受け取るため、リテーラは予約

証明証仲介許諾依頼作成部１８０３において予約証明証仲介許諾依頼を作成し、入出力制御部１８０１を介してプロバイダに送付する。

【０３１７】

予約証明証仲介許諾依頼作成部１８０３では、予約証明証仲介許諾依頼の各フィールドに以下の値を設定する。

【０３１８】

【表３５】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：予約証明証仲介許諾の依頼先であるプロバイダの識別子。

日時フィールド：現在の時刻。

予約証明証仲介許諾仕様フィールド：作成してもらう予約証明証仲介許諾に対するリテーラからの希望を記載する。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、予約証明証仲介許諾依頼作成部１８０３は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部１８０９にアクセスして入手する。

証明証フィールド：証明証記憶部１８１０に記憶している公開鍵証明証。

予約証明証仲介許諾依頼の予約証明証仲介許諾仕様フィールドに記載される予約証明証仲介許諾仕様の各フィールドには以下の値が設定される。

許諾者フィールド：予約証明証仲介許諾を発行してほしいプロバイダの識別子。

被許諾者フィールド：自分自身すなわちリテーラの識別子。

公開鍵識別子フィールド：予約証明証仲介許諾を発行してほしい検証用公開鍵に割り当てられた検証用公開鍵識別子。

希望予約条件限定情報フィールド：リテーラが予約証明証仲介許諾に記載してほしいと希望する予約条件限定情報。

【０３１９】

［予約証明証仲介許諾送付処理部］

予約証明証仲介許諾依頼作成部１８０３で予約証明証仲介許諾依頼が作成され

プロバイダに送付されると、その返信としてプロバイダから予約証明証仲介許諾送付が送信されてくる。予約証明証仲介許諾送付は、入出力制御部１８０１および処理選択部１８０２を経由して予約証明証仲介許諾送付処理部１８０５に送られ、そこで処理される。

【０３２０】

図２１は、本実施例のリテーラが持つ予約証明証仲介許諾送付処理部１８０５の動作を示すフローチャートである。予約証明証仲介許諾送付処理部１８０５の動作を図２１にしたがって説明する。

【０３２１】

まず、処理選択部１８０２から入力された予約証明証仲介許諾送付、および、該予約証明証仲介許諾送付に含まれる予約証明証仲介許諾のデジタル署名を検証する（２１０１）。検証鍵は予約証明証仲介許諾送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１１１から公開鍵証明証を取得してから署名の検証を行う。署名の検証のために、予約証明証仲介許諾送付処理部１８０５はデジタル署名の検証を専門に行う署名検証部を含んでいる。

【０３２２】

２１０１で、デジタル署名の検証に失敗した場合、エラー処理を行った後（２１０４）、終了する。

【０３２３】

２１０１で、デジタル署名の検証に成功した場合、予約証明証仲介許諾送付に含まれている予約証明証仲介許諾の作成者が正しいプロバイダであるかどうかが確認される（２１０２）。正しいプロバイダであるかどうかの判断基準にはいくつかバリエーションが有り得る。たとえば、予約証明証仲介許諾送付に含まれている予約証明証仲介許諾の発行者フィールドの値が、自分が依頼した予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の許諾者フィールドに記載されている識別子と一致するという基準はその一例である。予約証明証仲介許諾送付に含まれている予約証明証仲介許諾で予約証明証の仲介が許諾される検証用公開鍵と、該予約証明証仲介許諾の発行者との関係を確認したければ、センタが発行

した検証用公開鍵情報を確認すればよい。検証用公開鍵情報は公開可能な情報であるので、センタあるいはプロバイダが検証用公開鍵情報を自由にダウンロードできる形で公開することが可能である。

【０３２４】

２１０２の検査で、予約証明証仲介許諾の作成者が正しいプロバイダではなかった場合、エラー処理を行った後（２１０４）、終了する。

【０３２５】

２１０２の検査で、予約証明証仲介許諾の作成者が正しいプロバイダであると判断した場合、予約証明証仲介許諾ＤＢ１８０７に新しいエントリを追加する（２１０３）。新しいエントリの各属性には以下の値が設定される。

【０３２６】

【表３６】

予約証明証仲介許諾識別子属性：予約証明証仲介許諾送付に含まれる予約証明証仲介許諾の予約証明証仲介許諾識別子フィールドの値。

公開鍵識別子属性：予約証明証仲介許諾送付に含まれる予約証明証仲介許諾の公開鍵鍵識別子フィールドの値。

プロバイダ識別子属性：予約証明証仲介許諾送付に含まれる予約証明証仲介許諾の発行者フィールドの値。

予約証明証仲介許諾属性：予約証明証仲介許諾送付に含まれる予約証明証仲介許諾をＢＥＲにしたがってエンコードした結果。

プロバイダ証明証属性：予約証明証仲介許諾送付に含まれるプロバイダの署名の検証鍵を含む公開鍵証明証をＢＥＲにしたがってエンコードした結果。

【０３２７】

［予約証明証依頼処理部］

図２２は、本実施例のリテーラが持つ予約証明証依頼処理部１８０４の内部構成を示した図である。

【０３２８】

予約証明証依頼処理部１８０４は、消費者あるいは他のリテーラから送信された予約証明証依頼を処理し、センタへの予約証明証依頼を作成し、入出力制御部

１８０１経由でセンタへ送付する機能を持ち、処理制御部２２０１、署名検証部２２０２、エラーメッセージ作成部２２０３、予約証明証依頼作成部２２０４、署名作成部２２０５、予約条件作成部２２０６から構成される。

【０３２９】

予約証明証依頼処理部１８０４を構成する各部の役割を以下に述べる。

【０３３０】

処理制御部２２０１：処理選択部１８０２からの入力、入出力制御部１８０１への出力、予約証明証仲介許諾ＤＢ１８０７の参照、予約証明証仲介履歴ＤＢ１８０８へのエントリの追加の機能を担うとともに、予約証明証依頼の処理全体を制御する。

署名検証部２２０２：処理選択部１８０２から入力される予約証明証依頼のデジタル署名を検証する。

エラーメッセージ作成部２２０３：エラーメッセージを作成する。

予約証明証依頼作成部２２０４：センタへ送付する予約証明証依頼を作成する。予約証明証依頼にデジタル署名を添付するために署名作成部２２０５を呼び出す。さらに、リテーラの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部１８１０にアクセスする。

署名作成部２２０５：予約証明証依頼作成部２２０４で作成する予約証明証依頼のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部１８０９にアクセスする。

予約条件作成部２２０６：依頼する予約証明証に含まれるべき予約条件を作成する。

【０３３１】

図２３は、本実施例のリテーラが持つ予約証明証依頼処理部１８０４の処理制御部２２０１の動作を示すフローチャートである。処理制御部２２０１の動作を図２３にしたがって説明する。

【０３３２】

まず、処理選択部１８０２から入力された予約証明証依頼のデジタル署名を検証する（２３０１）。検証鍵は該予約証明証依頼の証明証フィールドに添付され

ているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１１１から公開鍵証明証を取得してから署名の検証を行う。

【０３３３】

署名の検証に失敗した場合、エラーメッセージ作成部２２０３でエラーメッセージを作成して入出力制御部１８０１に出力した後（２３０７）、終了する。

【０３３４】

署名の検証に成功した場合、入力された予約証明証依頼で予約証明証の仲介を依頼されている検証用公開鍵の仲介が許諾されているかどうかを検査する（２３０２）。予約証明証仲介許諾ＤＢ１８０７に、予約証明証依頼で依頼された検証用公開鍵に対する予約証明証仲介許諾が存在し、かつ予約証明証依頼に記載されている予約条件が、予約証明証仲介許諾ＤＢ１８０７に保持されている予約証明証仲介許諾に記載されている予約条件限定情報の範囲内である場合に許諾されていると判断する。

【０３３５】

２３０２の検査で仲介が許諾されていないと判断された場合、エラーメッセージ作成部２２０３でエラーメッセージを作成して入出力制御部１８０１に出力した後（２３０７）、終了する。

【０３３６】

２３０２の検査で仲介が許諾されていると判断された場合、予約証明証依頼を受け付けるかどうかを判断する（２３０３）。入力された予約証明証依頼の発信者である消費者やリテーラが信用できない場合は、ここで予約証明証依頼を受け付けないことを決定する。

【０３３７】

２３０３で予約証明証依頼を受け付けないと判断した場合、エラーメッセージ作成部２２０３でエラーメッセージを作成して入出力制御部１８０１に出力した後（２３０７）、終了する。

【０３３８】

２３０３で予約証明証依頼を受け付けると判断した場合、予約条件作成部２２０６を呼び出し、センタへ送付する予約証明証依頼に記載する予約条件を作成さ

せ、その結果を受けとる（２３０４）。予約条件作成部２２０６が作成する予約条件は、入力された予約証明証依頼に記載されている予約条件のままでもよいし、必要ならリテーラの裁量で適切なものに修正してもよい。

【０３３９】

予約条件が決まったら、処理中の予約証明証依頼に関する情報を保持したエントリを予約証明証仲介履歴ＤＢ１８０８に追加する（２３０５）。新しいエントリの各属性には以下の値が設定される。

【０３４０】

【表３７】

予約証明証識別子属性：この時点では値は設定されない。

公開鍵識別子属性：入力された予約証明証依頼に含まれる予約仕様の公開鍵識別子フィールドに記載されている値。

プロバイダ識別子属性：公開鍵識別子属性に設定された識別子で特定される検証用公開鍵情報のユーザであるプロバイダの識別子。該プロバイダの識別子は、予約証明証仲介許諾ＤＢを参照して得ることができる。すなわち、本ＤＢの公開鍵識別子属性に設定された識別子を予約証明証仲介許諾ＤＢの公開鍵識別子属性の値に持つ予約証明証仲介許諾ＤＢのエントリのプロバイダ識別子属性がそれにあたる。

消費者識別子属性：入力された予約証明証依頼に含まれる予約仕様の消費者識別子フィールドの値。

依頼者識別子属性：入力された予約証明証依頼の発信者フィールドの値。

予約条件属性：２３０４で決定した予約条件。

依頼日時属性：入力された予約証明証依頼の日時フィールドの値。

発信日時属性：この時点では値は設定されない。

【０３４１】

最後にセンタへ送付する予約証明証依頼を作成し、入出力制御部１８０１を介してセンタに送付し（２３０６）、終了する。センタへ送付する予約証明証依頼の各フィールドには以下の値が設定される。

【０３４２】

【表３８】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：センタの識別子。

日時フィールド：現在の日時。

予約内容フィールド：後述する予約仕様。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部２２０５を呼び出して署名値を作成させ、結果をこのフィールドに設定する。署名鍵は署名鍵記憶部１８０９にアクセスして入手する。

証明証フィールド：証明証記憶部１８１０に記憶している公開鍵証明証。

【０３４３】

予約内容フィールドに記載される予約仕様の各フィールドには、以下の値が記載される。

【０３４４】

【表３９】

公開鍵識別子フィールド：入力された予約証明証依頼に含まれる予約仕様の公開鍵識別子フィールドに記載されている値。

消費者識別子フィールド：入力された予約証明証依頼に含まれる予約仕様の消費者識別子フィールドに記載されている値。

予約条件フィールド：２３０４で決定した予約条件。

予約証明証仲介許諾フィールド：予約証明証仲介許諾ＤＢ１８０７に保持されている、予約証明証依頼で予約証明証の発行を依頼された検証用公開鍵に対する予約証明証仲介許諾。

【０３４５】

［予約証明証送付処理部］

図２４は、本実施例のリテーラが持つ予約証明証送付処理部１８０６の内部構成を示した図である。

【０３４６】

予約証明証送付処理部１８０６は、センタあるいは他のリテーラからの送信さ

れた予約証明証送付を処理し、予約証明証の依頼者に送付する予約証明証送付を作成し、入出力制御部１８０１経由で該依頼者に送付する機能を持ち、処理制御部２４０１、署名検証部２４０２、エラーメッセージ作成部２４０３、予約証明証送付作成部２４０４、署名作成部２４０５から構成される。

【０３４７】

予約証明証送付処理部１８０６を構成する各部の役割を以下に述べる。

【０３４８】

処理制御部２４０１：処理選択部１８０２からの入力、入出力制御部１８０１への出力、予約証明証仲介履歴ＤＢ１８０８のエントリ更新の機能を担うとともに、予約証明証送付の処理全体を制御する。

署名検証部２４０２：処理選択部１８０２から入力される予約証明証送付、および予約証明証送付に含まれる予約証明証のデジタル署名を検証する。

エラーメッセージ作成部２４０３：エラーメッセージを作成する。

予約証明証送付作成部２４０４：予約証明証の依頼者に送付する予約証明証送付を作成する。新たに作成する予約証明証送付にデジタル署名を添付するために署名作成部２４０５を呼び出す。さらに、リテーラの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部１８１０にアクセスする。

署名作成部２４０５：予約証明証送付作成部２４０４で作成する予約証明証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部１８０９にアクセスする。

【０３４９】

図２５は、本実施例のリテーラが持つ予約証明証送付処理部１８０６の処理制御部２４０１の動作を示すフローチャートである。処理制御部２４０１の動作を図２５にしたがって説明する。

【０３５０】

まず、処理選択部１８０２から入力された予約証明証送付および該予約証明証送付に含まれる予約証明証のデジタル署名を検証する（２５０１）。検証鍵は該予約証明証送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１１１から公開鍵

証明証を取得してから署名の検証を行う。

【０３５１】

署名の検証に失敗した場合、エラーメッセージ作成部２４０３でエラーメッセージを作成して入出力制御部１８０１に出力した後（２５０４）、終了する。

【０３５２】

署名の検証に成功した場合、入力された予約証明証送付で送付された内容にしたがって、予約証明証仲介履歴ＤＢ１８０８のエントリを更新する（２５０２）。更新されるエントリは、入力された予約証明証送付に対応する予約証明証依頼を処理した時に追加されたエントリであり、エントリの公開鍵識別子属性、消費者識別子属性の値が、それぞれ入力された予約証明証送付に含まれる予約証明証の公開鍵識別子フィールド、受領者フィールドの値と一致し、該エントリの予約証明証識別子属性と発信日時属性の値が設定されていないものである。

【０３５３】

更新対象のエントリの各属性は以下のように更新される。

【０３５４】

【表４０】

予約証明証識別子属性：入力された予約証明証送付に含まれる予約証明証の予約証明証識別子フィールドの値。

公開鍵識別子属性：変化なし。

プロバイダ識別子属性：変化なし。

消費者識別子属性：変化なし。

依頼者識別子属性：変化なし。

予約条件属性：入力された予約証明証送付に含まれる予約証明証の予約条件フィールドの値。

依頼日時属性：変化なし。

発信日時属性：現在の時刻。

【０３５５】

最後に、予約証明証の依頼者に送付する新たな予約証明証送付を作成し、入出力制御部１８０１を介して予約証明証の依頼者に送付し（２５０３）、終了する

。新たに作成される予約証明証送付の各フィールドには以下の値が設定される。

【０３５６】

【表４１】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：２５０２で更新された予約証明証仲介履歴ＤＢ１８０８のエントリの依頼者識別子属性の値。

日時フィールド：２５０２で更新された予約証明証仲介履歴ＤＢ１８０８のエントリの発信日時属性の値。

予約証明証フィールド：入力された予約証明証送付に含まれる予約証明証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部２４０５を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部１８１０に記憶している公開鍵証明証と、入力された予約証明証送付の証明証フィールドに含まれる証明証のうち、該予約証明証送付に含まれる予約証明証のデジタル署名を検証できる検証鍵を含む公開鍵証明証。

【０３５７】

［予約証明証依頼処理の課金・決済］

本実施例のリテーラは、予約証明証依頼の処理の過程で予約証明証発行料金の課金あるいは決済を行うことができる。課金あるいは決済の処理は、消費者からの予約証明証依頼をうけた後、センタに予約証明証依頼を送付する前に行われる。

【０３５８】

課金の場合は、予約証明証依頼の処理の過程で、消費者毎に予約証明証発行料金を加算しておき、後に消費者に対して請求する。そのため、本実施例のリテーラは、消費者毎に現在の予約証明証発行料金高を保持するデータベースをもっている。

【０３５９】

本実施例のリテーラは、予約証明証依頼の処理のたび毎に予約証明証発行料金

の決済を行うこともできる。決済の方法としては、消費者が所持するクレジットカードによる決済や、プリペイドの方式等種々のものが利用可能であるが、いずれも、消費者からの予約証明証依頼をうけた後、決済が終了した事が確認されてから、センタに予約証明証依頼を送付する。

【０３６０】

また、予約証明証発行料金を予約証明証の検証時にプロバイダに回収させる事もできる。

【０３６１】

この場合、予約証明証に含まれる予約条件に料金情報を記載しておき、プロバイダが設置している予約証明証検証機器が予約証明証を検証する際に、予約証明証に含まれる予約条件が満たされているかどうかの判定の際に、料金が入手あるいは自動的に徴収されたことを確認すればよい。

【０３６２】

［リテーラが発行する履歴情報］

本実施例のリテーラは予約証明証仲介の履歴情報をプロバイダに送付する事ができる。

【０３６３】

プロバイダに渡される予約証明証仲介の履歴情報は、そのプロバイダに割り当てられた検証用公開鍵に対応する予約証明証の仲介についての情報であり、予約証明証仲介プロバイダ用履歴作成部１８１１で作成され、入出力制御部１８０１を介してプロバイダに送付される。この履歴は、リテーラがプロバイダに送付するマージンの額に対する根拠となる。

【０３６４】

予約証明証仲介プロバイダ用履歴作成部１８１１は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証仲介履歴ＤＢ１８０８から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その予約証明証識別子属性、公開鍵識別子属性、予約条件属性、依頼日時属性、発信日時属性の値を取り出す。本実施例では、履歴を作

成するプロバイダの識別子と履歴作成の対象期間の指定はリテーラのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【０３６５】

また、本実施例のリテーラは予約証明証仲介の履歴情報を予約証明証仲介の依頼者にも送付する事ができる。

【０３６６】

依頼者に渡される予約証明証仲介の履歴情報は、その依頼者から依頼された予約証明証の仲介についての情報であり、予約証明証仲介依頼者用履歴作成部１８１２で作成され、入出力制御部１８０１を介して依頼者に送付される。この履歴は、リテーラが依頼者に対して手数料の請求を行う場合の根拠となる。

【０３６７】

予約証明証仲介依頼者用履歴作成部１８１２は、履歴を作成する依頼者の識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証仲介履歴ＤＢ１８０８から、依頼者識別子属性の値が指定された依頼者の識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その予約証明証識別子属性、公開鍵識別子属性、プロバイダ識別子属性、消費者識別子属性、予約条件属性、依頼日時属性、発信日時属性の値を取り出す。本実施例では、履歴を作成する依頼者の識別子と履歴作成の対象期間の指定はリテーラのオペレータから受けるが、インターネット経由で依頼者から入力されるように構成してもよい。

【０３６８】

上記の履歴情報のプロバイダや依頼者への送付方法は、電子メールでもよいし、ＷＷＷベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

【０３６９】

[消費者端末の構成]

図２６は、本実施例の消費者端末の構成図である。

【０３７０】

本実施例の消費者端末は、インターネットを介してリテーラから予約証明証を受け取る。予約証明証依頼を作成してインターネットを介してリテーラに送付する機能と、インターネットを介してリテーラから送付される予約証明証送付を処理する機能を持つ。消費者端末は、入出力制御部２６０２、予約証明証依頼作成部２６０３、予約証明証送付処理部２６０４、署名鍵記憶部２６０５、証明証記憶部２６０６、携帯型記憶装置制御部２６０７から構成され、入出力制御部２６０２を介してインターネットに接続されているとともに、携帯型記憶装置制御部２６０７を介して携帯型記憶装置と接続されている。

【０３７１】

本実施例の消費者端末の各部の役割を以下に述べる。

【０３７２】

入出力制御部２６０２：インターネットを介したデータの入力を受け付けるとともに、予約証明証依頼作成部２６０３が作成した予約証明証依頼をインターネットを介して出力する。インターネットからの入出力制御部２６０２への入力、あるいは、入出力制御部２６０２からインターネットへの出力の方法としては、他のエンティティが用意しているＷＷＷサイトにアクセスして消費者端末が作成したデータを送るもの、あるいは電子メールシステムと入出力制御部２６０２を自動的にあるいは人手によって連動させるものなどが使用できる。

予約証明証依頼作成部２６０３：予約証明証依頼を作成し、入出力制御部２６０２を介してリテーラに送付する。予約証明証依頼の作成の過程で、署名鍵記憶部２６０５と証明証記憶部２６０６にアクセスするとともに、携帯型記憶装置制御部２６０７を介して携帯型記憶装置２６０８にアクセスする。

予約証明証送付処理部２６０４：リテーラからの予約証明証送付を処理し、該予約証明証送付に含まれている予約証明証を携帯型記憶装置制御部２６０７を介して携帯型記憶装置２６０８に記録する。

署名鍵記憶部２６０５：消費者端末が作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部２６０６：署名鍵記憶部２６０５に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

携帯型記憶装置制御部２６０７：携帯型記憶装置２６０８へのデータの書込みとアクセスを行う。

【０３７３】

本実施例では、予約証明証依頼にデジタル署名を施す場合に使用する署名鍵や、その署名鍵で作成した署名を検証する検証鍵を含む公開鍵証明証は、消費者端末が保持しているものとしたが、これらが携帯型記憶装置に保持されているように構成してもよい。

【０３７４】

[予約証明証依頼作成部]

本実施例の消費者端末は、該端末を利用している消費者が予約したい物品やサービスがある場合、その物品やサービスの予約証明証の仲介を依頼する予約証明証依頼を予約証明証依頼作成部２６０３で作成し、入出力制御部２６０２を介してリテーラに送付する。

【０３７５】

予約証明証依頼作成部２６０３では、予約証明証依頼の各フィールドに以下の値を設定する。

【０３７６】

【表４２】

発信者フィールド：自分自身すなわち消費者端末の識別子。

受信者フィールド：リテーラの識別子。

日時フィールド：現在の時刻。

予約内容フィールド：後述する予約仕様。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、予約証明証依頼作成部２６０３は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部２６０５にアクセスして入手する。

証明証フィールド：証明証記憶部２６０６に記憶している公開鍵証明証。

予約内容フィールドに指定される予約仕様の各フィールドには以下の値が設定さ

れる。

公開鍵識別子フィールド：予約したい物品やサービスに割り当てられている検証用公開鍵の識別子。

消費者識別子フィールド：消費者端末を使用している消費者の識別子。消費者識別子は携帯型記憶装置２６０８に記憶されており、予約証明証依頼作成部２６０３は、携帯型記憶装置制御部２６０７を介して携帯型記憶装置２６０８から消費者識別子を入手する。

予約条件フィールド：消費者の希望等を反映した適切なものを予約証明証依頼作成部２６０３が決定して設定。

予約証明証仲介許諾フィールド：設定しない。

【０３７７】

[予約証明証送付処理部]

予約証明証依頼作成部２６０３で予約証明証依頼が作成されリテーラに送付されると、その返信としてリテーラから予約証明証送付が送信されてくる。予約証明証送付は、入出力制御部２６０２を経由して予約証明証送付処理部２６０４に入力され、そこで処理される。

【０３７８】

図２７は、本実施例の消費者端末が持つ予約証明証送付処理部２６０４の動作を示すフローチャートである。予約証明証送付処理部２６０４の動作を図２７にしたがって説明する。

【０３７９】

まず、入力された予約証明証送付および該予約証明証送付に含まれる予約証明証のデジタル署名を検証する（２７０１）。検証鍵は検証用公開情報送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、ＣＡ１１１から公開鍵証明証を取得してから署名の検証を行う。

【０３８０】

２７０１で、デジタル署名の検証に失敗した場合、エラー処理を行った後（２７０４）、終了する。

【０３８１】

２７０１で、デジタル署名の検証に成功した場合、入力された予約証明証送付に含まれる予約証明証が、現在消費者端末を使用している消費者向けのものかどうかが検査される（２７０２）。検査は、携帯型記憶装置制御部２６０７を介して携帯型記憶装置２６０８から入手した消費者識別子と、入力された予約証明証送付に含まれる予約証明証の受領者フィールドの値が一致するかどうかで行われる。

【０３８２】

２７０２の検査で、入力された予約証明証送付に含まれる予約証明証が現在消費者端末を使用している消費者向けのものでないと判断された場合、エラー処理を行った後（２７０４）、終了する。

【０３８３】

２７０２の検査で、入力された予約証明証送付に含まれる予約証明証が現在消費者端末を使用している消費者向けのものであると判断された場合、該予約証明証を携帯型記憶装置制御部２６０７を介して携帯型記憶装置２６０８に記録し（２７０３）、終了する。

【０３８４】

【発明の効果】

以上説明したようにこの発明によれば予約販売を行う際に予約販売業者は証明証を発行するリソースを自ら構築する必要がない。

【図面の簡単な説明】

【図１】　本発明を適用した実施例の構成図である。

【図２】本発明を適用したセンタの構成図である。

【図３】本発明を適用したセンタの動作を示すフローチャートである。

【図４】本発明を適用したセンタが持つ検証用公開情報依頼処理部の内部構成を示した図である。

【図５】本発明を適用したセンタが持つ検証用公開情報依頼処理部の処理制御部の動作を示すフローチャートである。

【図６】本発明を適用したセンタが持つプロバイダＤＢの構造を示した図で

ある。

【図７】本発明を適用したセンタが持つ公開鍵ペアＤＢの構造を示した図である。

【図８】本発明を適用したセンタが持つリテーラＤＢの構造を示した図である。

【図９】本発明を適用したセンタが持つ消費者ＤＢの構造を示した図である。

【図１０】本発明を適用したセンタが持つ予約証明証発行履歴ＤＢの構造を示した図である。

【図１１】本発明を適用したセンタが持つ予約証明証依頼処理部の内部構成を示した図である。

【図１２】本発明を適用したセンタが持つ予約証明証依頼処理部の処理制御部の動作を示すフローチャートである。

【図１３】本発明を適用したプロバイダの構成図である。

【図１４】本発明を適用したプロバイダが持つ検証用公開鍵ＤＢの構造を示した図である。

【図１５】本発明を適用したプロバイダが持つ検証用公開情報送付処理部の動作を示すフローチャートである。

【図１６】本発明を適用したプロバイダが持つ予約証明証仲介許諾依頼処理部の内部構成を示した図である。

【図１７】本発明を適用したプロバイダが持つ予約証明証仲介許諾依頼処理部の処理制御部の動作を示すフローチャートである。

【図１８】本発明を適用したリテーラの構成図である。

【図１９】本発明を適用したリテーラが持つ予約証明証仲介許諾ＤＢの構造を示した図である。

【図２０】本発明を適用したリテーラが持つ予約証明証仲介履歴ＤＢの構造を示した図である。

【図２１】本発明を適用したリテーラが持つ予約証明証仲介許諾送付処理部の動作を示すフローチャートである。

【図２２】本発明を適用したリテーラが持つ予約証明証依頼処理部の内部構成を示した図である。

【図２３】本発明を適用したリテーラが持つ予約証明証依頼処理部の処理制御部の動作を示すフローチャートである。

【図２４】本発明を適用したリテーラが持つ予約証明証送付処理部の内部構成を示した図である。

【図２５】本発明を適用したリテーラが持つ予約証明証送付処理部の処理制御部の動作を示すフローチャートである。

【図２６】本発明を適用した消費者端末の構成図である。

【図２７】本発明を適用した消費者端末が持つ予約証明証送付処理部の動作を示すフローチャートである。

【図２８】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第１の構成例を示した図である。

【図２９】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第１の構成例における、予約証明証の検証の際の予約証明証検証機器と携帯型記憶装置の動作を示すフローチャートである。

【図３０】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第２の構成例を示した図である。

【図３１】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第２の構成例における、予約証明証の検証の際の予約証明証検証機器と携帯型記憶装置の動作を示すフローチャートである。

【図３２】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第３の構成例を示した図である。

【図３３】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第３の構成例における、予約証明証の検証の際の予約証明証検証機器と携帯型記憶装置の動作を示すフローチャートである。

【図３４】本発明を適用したプロバイダが持つ予約証明証仲介許諾発行履歴ＤＢの構造を示した図である。

【符号の説明】

１０１　インターネット

１０２　予約証明証発行センタ

１０３、１０４　リテーラ

１０５、１０７　プロバイダ

１０６、１０８　検証機器

１０９　消費者端末

１１０　携帯型記憶装置

１１１　認証局（Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）

２０１　入出力制御部

２０２　処理選択部

２０３　検証用公開鍵情報依頼処理部

２０４　予約証明証依頼処理部

２０５　プロバイダＤＢ

２０６　公開鍵ペアＤＢ

２０７　リテーラＤＢ

２０８　消費者ＤＢ

２０９　予約証明証発行履歴ＤＢ

２１０　署名鍵記憶部

２１１　証明証記憶部

２１２　予約証明証発行プロバイダ用履歴作成部

２１３　予約証明証発行リテーラ用履歴作成部

２１４　検証用公開鍵情報発行履歴作成部

４０１　処理制御部

４０２　署名検証部

４０３　公開鍵ペア作成部

４０４　公開鍵ペア識別子作成部

４０５　検証用公開鍵情報作成部

４０６　検証用公開鍵情報送付作成部

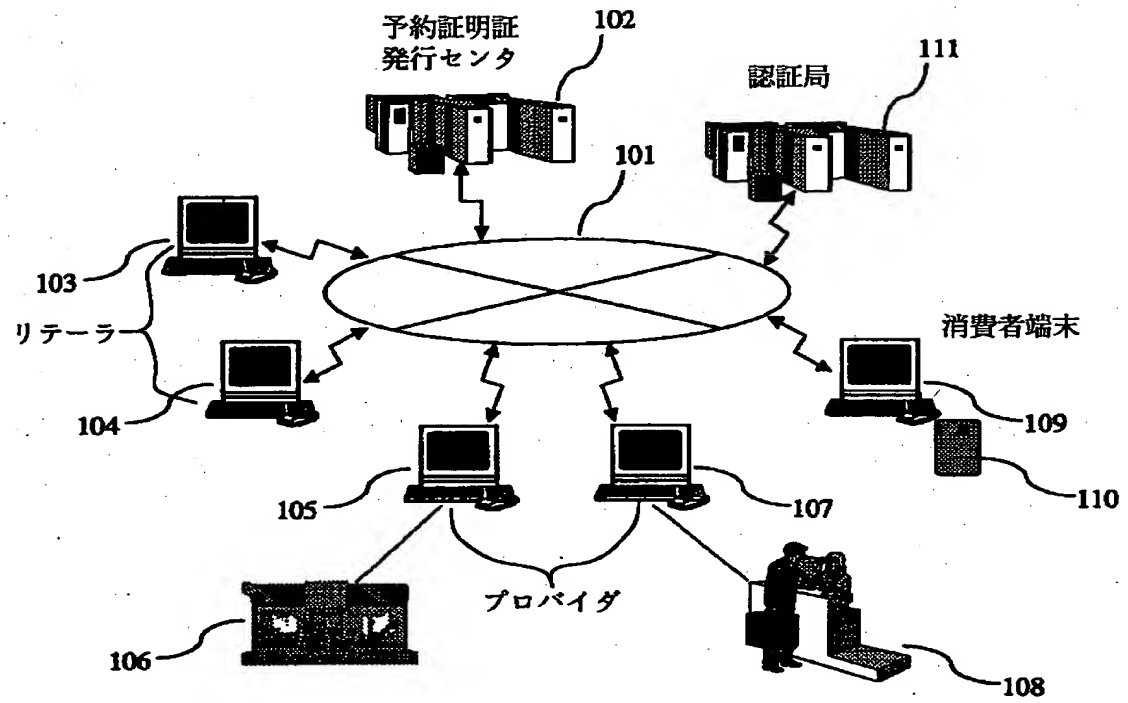
４０７　エラーメッセージ作成部

４０８　署名作成部
１１０１　処理制御部
１１０２　署名検証部
１１０３　予約証明証仲介許諾内容確認部
１１０４　予約証明証識別子作成部
１１０５　予約証明証作成部
１１０６　予約証明証送付作成部
１１０７　エラーメッセージ作成部
１１０８　署名作成部
１１０９　予約値作成部
１１１０　予約条件作成部
１３０１　入出力制御部
１３０２　処理選択部
１３０３　検証用公開鍵情報依頼作成部
１３０４　検証用公開鍵情報送付処理部
１３０５　予約証明証仲介許諾依頼処理部
１３０６　検証用公開鍵ＤＢ
１３０７　署名鍵記憶部
１３０８　証明証記憶部
１３０９　予約証明証仲介許諾発行履歴ＤＢ
１３１０　予約証明証仲介許諾発行履歴作成部
１８０１　入出力制御部
１８０２　処理選択部
１８０３　予約証明証仲介許諾依頼作成部
１８０４　予約証明証依頼処理部
１８０５　予約証明証仲介許諾送付処理部
１８０６　予約証明証送付処理部
１８０７　予約証明証仲介許諾ＤＢ
１８０８　予約証明証仲介履歴ＤＢ

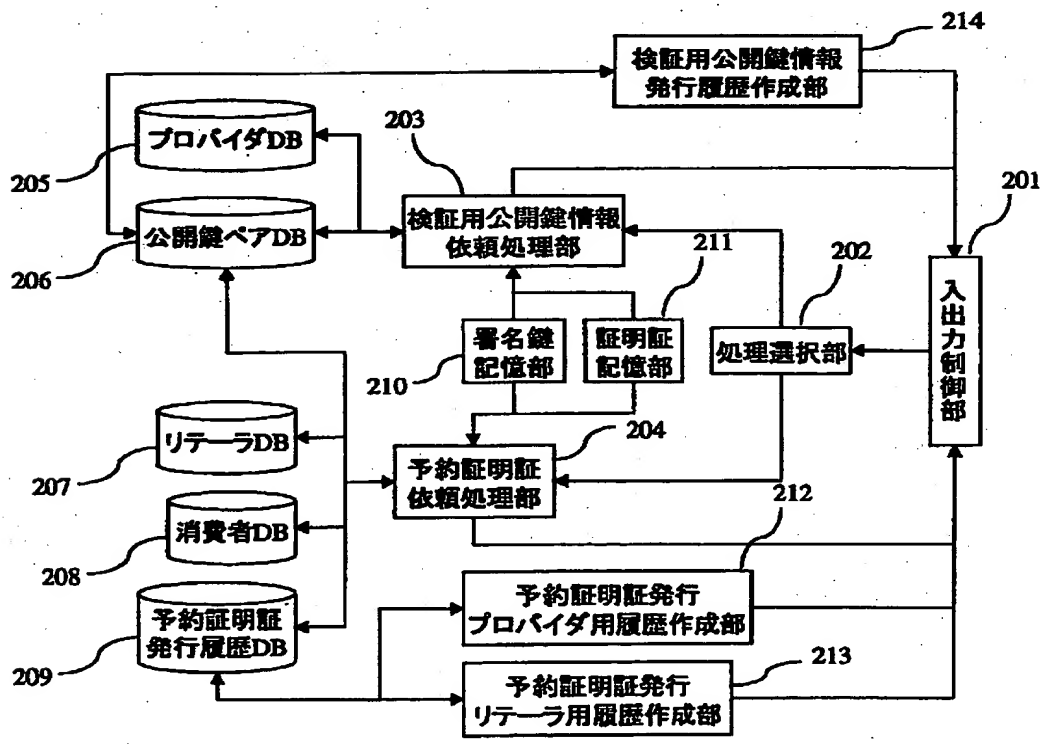
１８０９　署名鍵記憶部
１８１０　証明証記憶部
１８１１　予約証明証仲介プロバイダ用履歴作成部
１８１２　予約証明証仲介依頼者用履歴作成部
２６０１　消費者端末
２６０２　入出力制御部
２６０３　予約証明証依頼作成部
２６０４　予約証明証送付処理部
２６０５　署名鍵記憶部
２６０６　証明証記憶部
２６０７　携帯型記憶装置制御部
２６０８　携帯型記憶装置
２８０１　予約証明証検証機器
２８０２　条件指定記憶部
２８０３　チャレンジ生成部
２８０４　公開鍵情報記憶部
２８０５　レスポンス検査部
２８０６　携帯型記憶装置制御部
２８１１　携帯型記憶装置
２８１２　入出力制御部
２８１３　消費者秘密情報記憶部
２８１４　レスポンス計算部
２８１５　予約条件判定部
２８１６　予約証明証記憶部

【書類名】　　図面

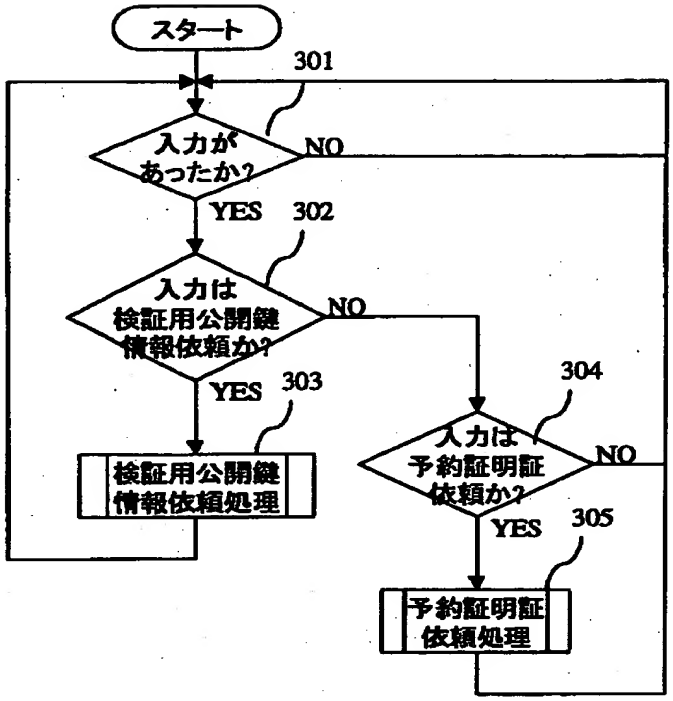
【図１】


予約証明証
発行センタ
102
認証局
111
101
103
リテーラ
104
消費者端末
109
110
105
107
プロバイダ
106
108

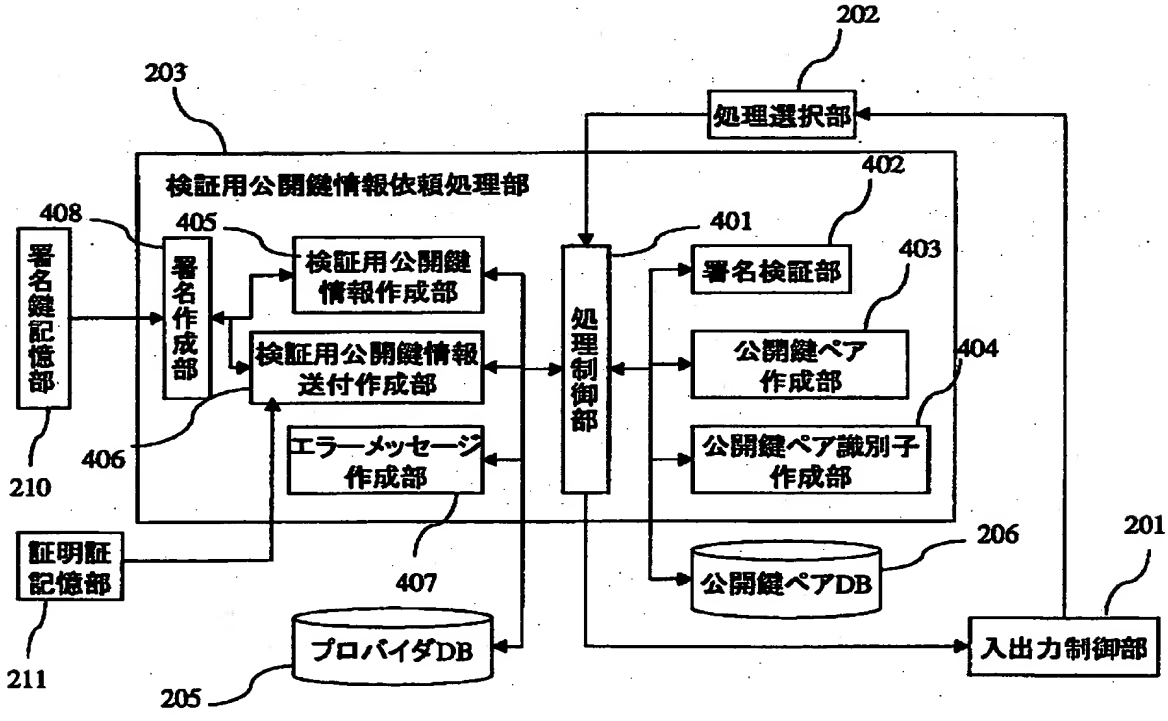
【図２】


214
検証用公開鍵情報
発行履歴作成部
プロバイダDB
205
203
201
公開鍵ペアDB
206
検証用公開鍵情報
依頼処理部
211
202
署名鍵
記憶部
210
証明証
記憶部
処理選択部
入出力制御部
リテーラDB
207
204
予約証明証
依頼処理部
212
消費者DB
208
予約証明証
発行履歴DB
209
予約証明証発行
プロバイダ用履歴作成部
213
予約証明証発行
リテーラ用履歴作成部

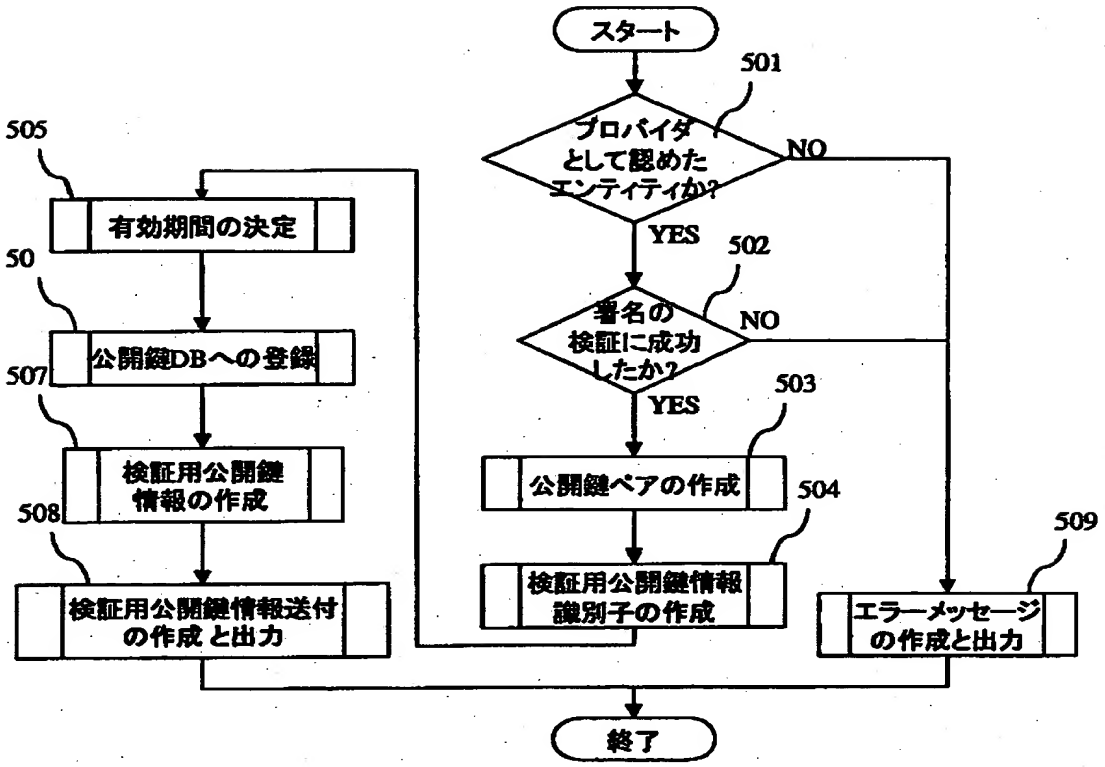
【図３】


スタート
301
入力があったか?
NO
YES
302
入力は検証用公開鍵情報依頼か?
NO
YES
303
検証用公開鍵情報依頼処理
304
入力は予約証明証依頼か?
NO
YES
305
予約証明証依頼処理

【図４】


202
処理選択部
203
検証用公開鍵情報依頼処理部
408
署名鍵記憶部
405
署名作成部
検証用公開鍵情報作成部
検証用公開鍵情報送付作成部
エラーメッセージ作成部
406
210
証明証記憶部
211
407
プロバイダDB
205
401
処理制御部
402
署名検証部
403
公開鍵ペア作成部
404
公開鍵ペア識別子作成部
206
公開鍵ペアDB
201
入出力制御部

【図５】



【図６】

プロバイダ識別子
PRV10001
PRV10002
PRV10003
...

【図７】

公開鍵識別子	法数	公開鍵	秘密鍵	プロバイダ識別子	有効期間開始	有効期間終了	発行日
PK00001	10110...	11001...	10101...	PRV10001	2000.1.1	2001.1.1	2000.12.1
PK00002	10010...	11110...	11011...	PRV10003	1999.3.5	2000.2.3	2000.1.2
PK00003	11111...	10000...	10101...	PRV10001	1999.11.1	2000.5.1	2000.3.1
...	...	...	...	...	...	...	...

【図８】

リテーラ識別子
RTL10001
RTL10002
RTL10003
...

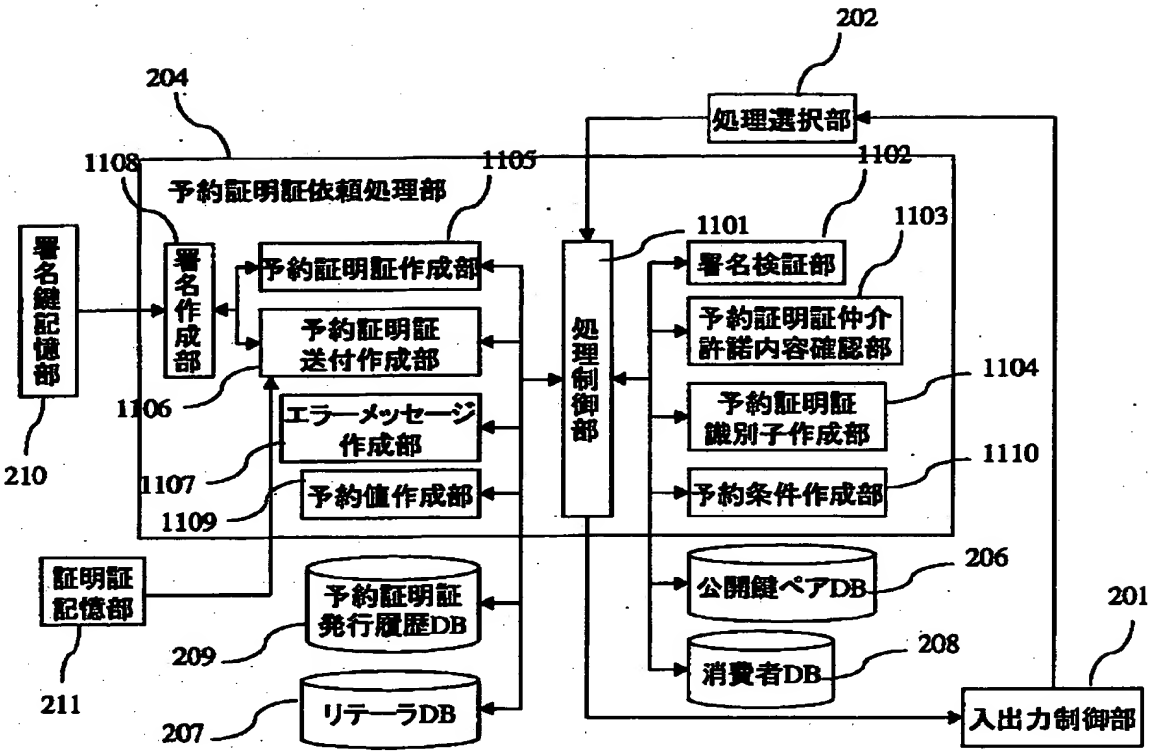
【図９】

消費者識別子	消費者秘密情報
CNS10001	10110...
CNS10002	11000...
CNS10003	01110...
...	...

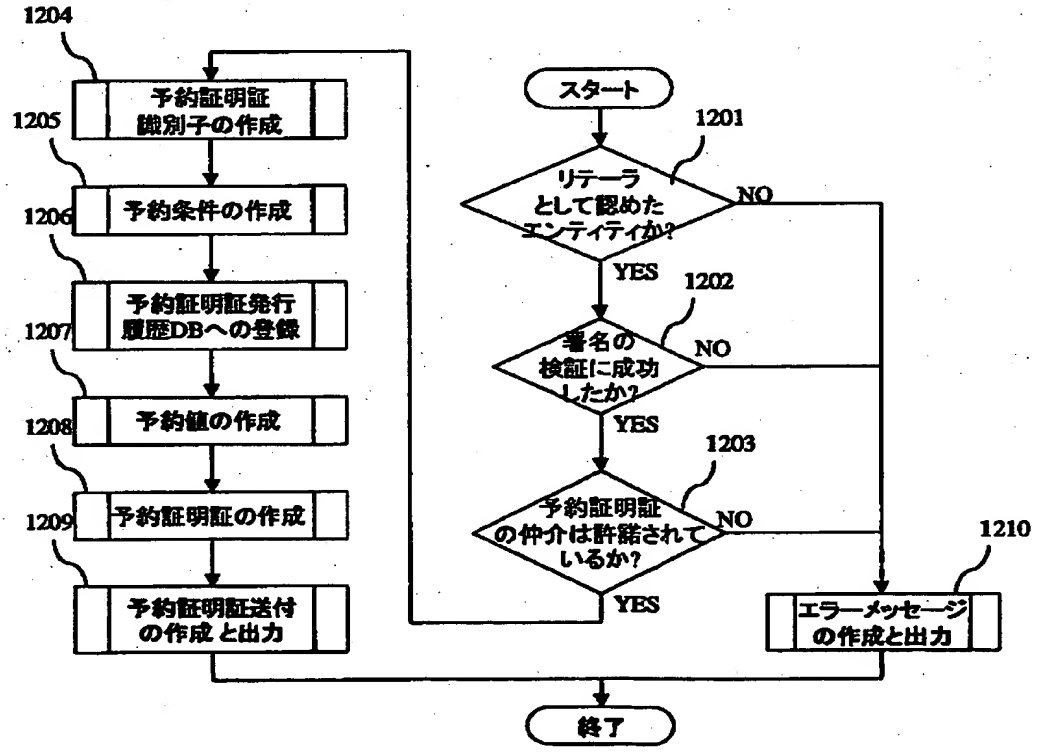
【図１０】

公開鍵識別子	プロバイダ識別子	消費者識別子	仲介者識別子	予約条件	発行日
PK00001	PRV10001	CNS10001	RTL10002	2F34A...	2000.2.1
PK00002	PRV10003	CNS10001	RTL10002	44FBC...	1999.4.16
PK00002	PRV10003	CNS10003	RTL10001	5AAB1...	1999.11.12
...	...	...	...	...	...

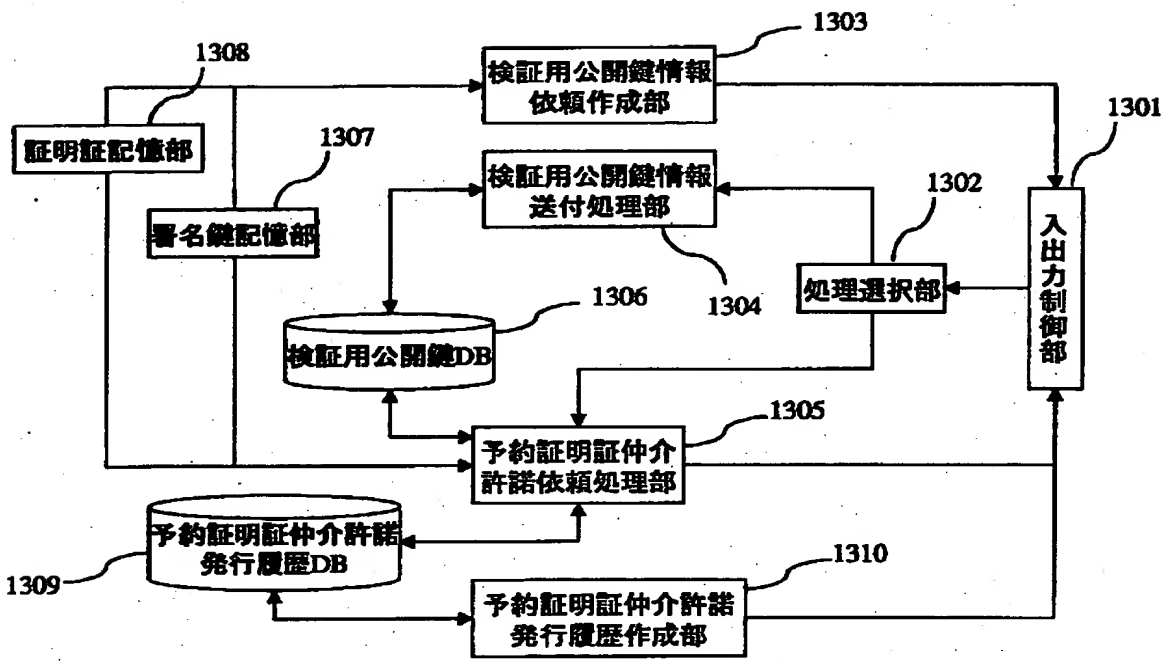
【図１１】


202
処理選択部
204
1108
予約証明証依頼処理部
1105
1102
1101
1103
署名鍵記憶部
署名作成部
予約証明証作成部
署名検証部
予約証明証送付作成部
処理制御部
予約証明証仲介許諾内容確認部
1106
1104
エラーメッセージ作成部
予約証明証識別子作成部
210
1107
1110
予約値作成部
予約条件作成部
1109
証明証記憶部
予約証明証発行履歴DB
公開鍵ペアDB
206
201
209
208
消費者DB
211
リテーラDB
207
入出力制御部

【図１２】


1204
予約証明証識別子の作成
1205
予約条件の作成
1206
予約証明証発行履歴DBへの登録
1207
予約値の作成
1208
予約証明証の作成
1209
予約証明証送付の作成と出力
スタート
1201
リテーラとして認めたエンティティか?
NO
YES
1202
署名の検証に成功したか?
NO
YES
1203
予約証明証の仲介は許諾されているか?
NO
YES
1210
エラーメッセージの作成と出力
終了

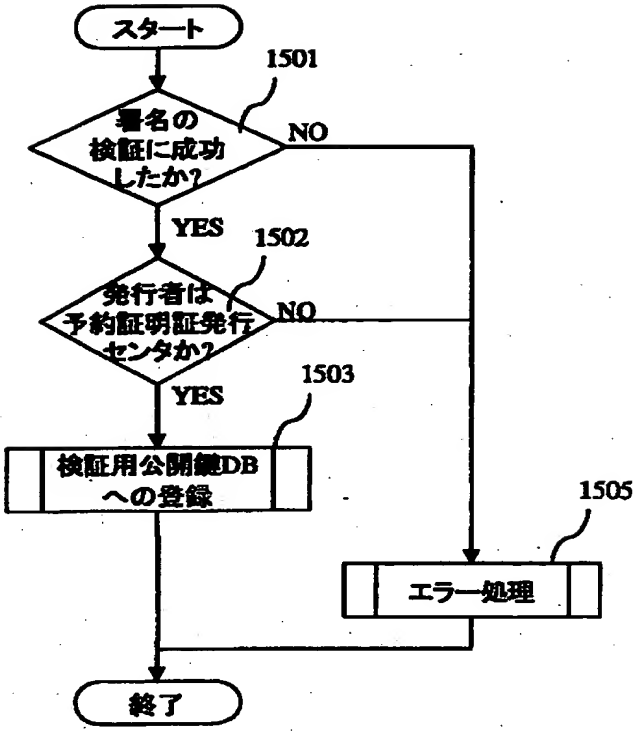
【図１３】



【図１４】

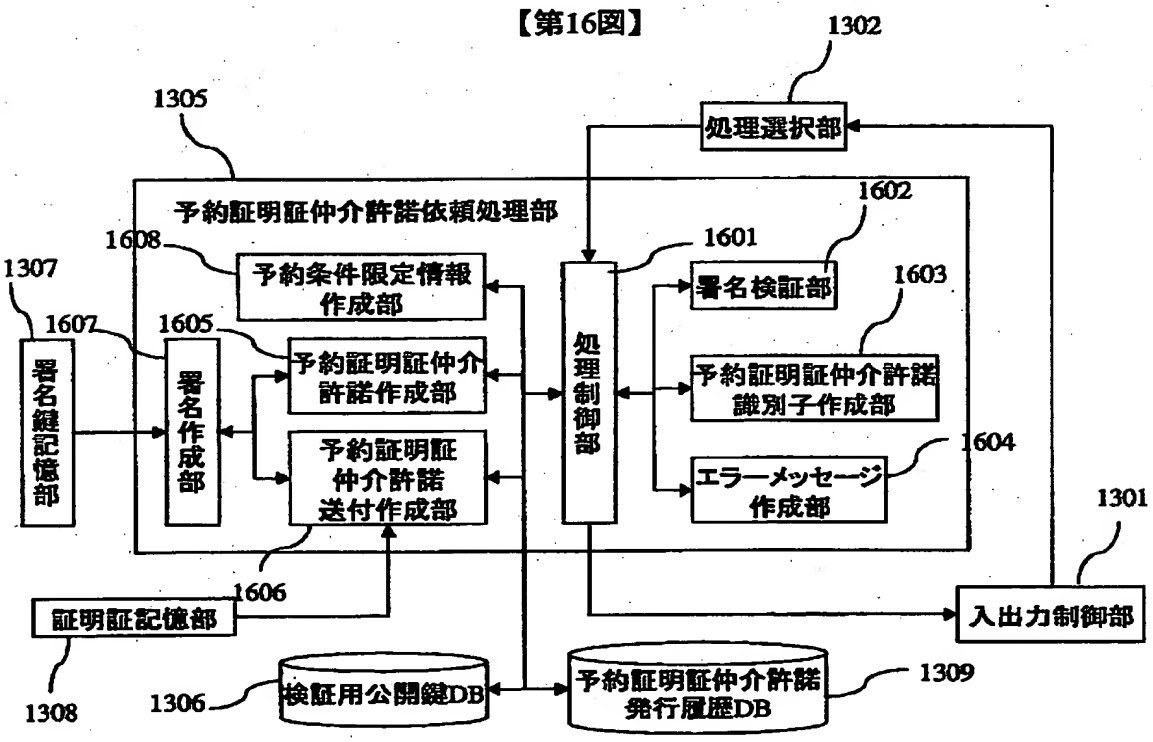
公開鍵識別子	法数	公開鍵	有効期間開始	有効期間終了	用途
PK00001	10110...	11001...	2000.1.1	2001.1.1	TT3 鑑賞券
PK00003	11111...	10000...	1999.11.1	2000.5.1	Millennium Watch Black
PK00007	11000...	10110...	1999.8.1	2000.2.1	GWJr コンサート 2000.1.15S 席
...	...	...	...	...	...

【図１５】

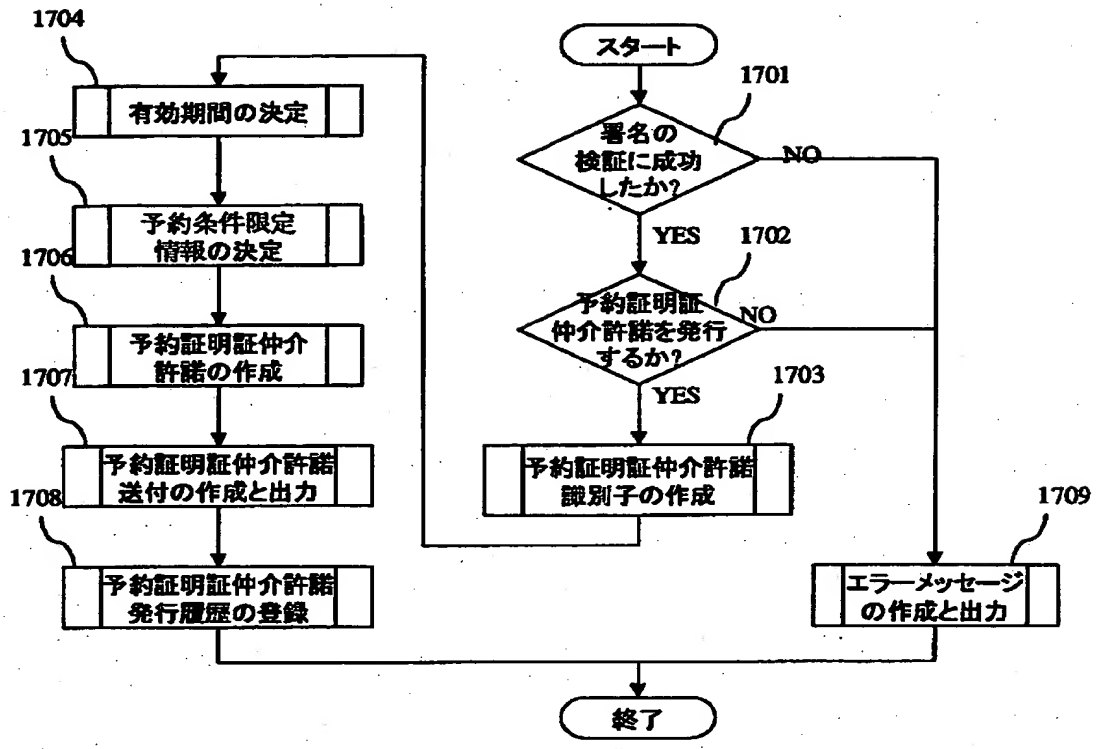

スタート
1501
署名の検証に成功したか?
NO
YES
1502
発行者は予約証明証発行センタか?
NO
YES
1503
検証用公開鍵DBへの登録
1505
エラー処理
終了

【図１６】

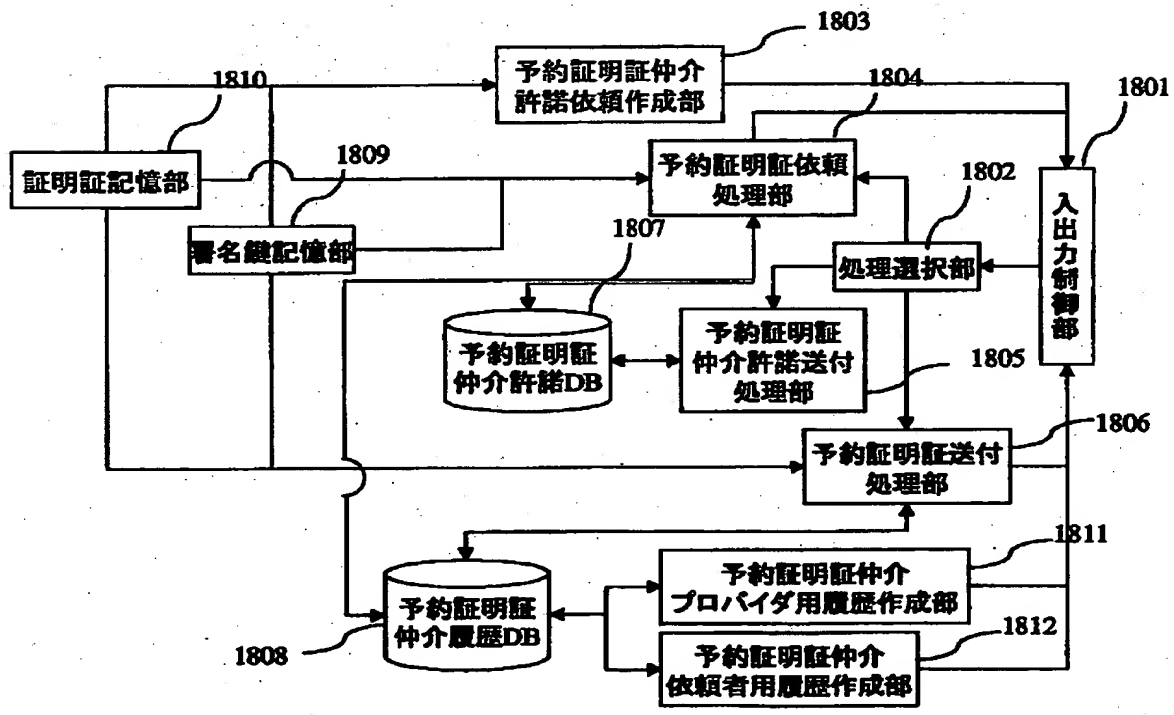
【第16図】


1302
処理選択部
1305
予約証明証仲介許諾依頼処理部
1602
1601
1608
予約条件限定情報作成部
1307
1607
1605
署名鍵記憶部
署名作成部
予約証明証仲介許諾作成部
予約証明証仲介許諾送付作成部
処理制御部
署名検証部
1603
予約証明証仲介許諾識別子作成部
エラーメッセージ作成部
1604
1301
1606
証明証記憶部
入出力制御部
1308
1306
検証用公開鍵DB
予約証明証仲介許諾発行履歴DB
1309

【図１７】


スタート
1701
署名の検証に成功したか?
NO
YES
1702
予約証明証仲介許諾を発行するか?
NO
YES
1703
予約証明証仲介許諾識別子の作成
1704
有効期間の決定
1705
予約条件限定情報の決定
1706
予約証明証仲介許諾の作成
1707
予約証明証仲介許諾送付の作成と出力
1708
予約証明証仲介許諾発行履歴の登録
1709
エラーメッセージの作成と出力
終了

【図１８】


1803
予約証明証仲介許諾依頼作成部
1810
1804
1801
証明証記憶部
1809
予約証明証依頼処理部
1802
署名鍵記憶部
1807
処理選択部
入出力制御部
予約証明証仲介許諾DB
予約証明証仲介許諾送付処理部
1805
1806
予約証明証送付処理部
1811
予約証明証仲介プロバイダ用履歴作成部
予約証明証仲介履歴DB
1808
1812
予約証明証仲介依頼者用履歴作成部

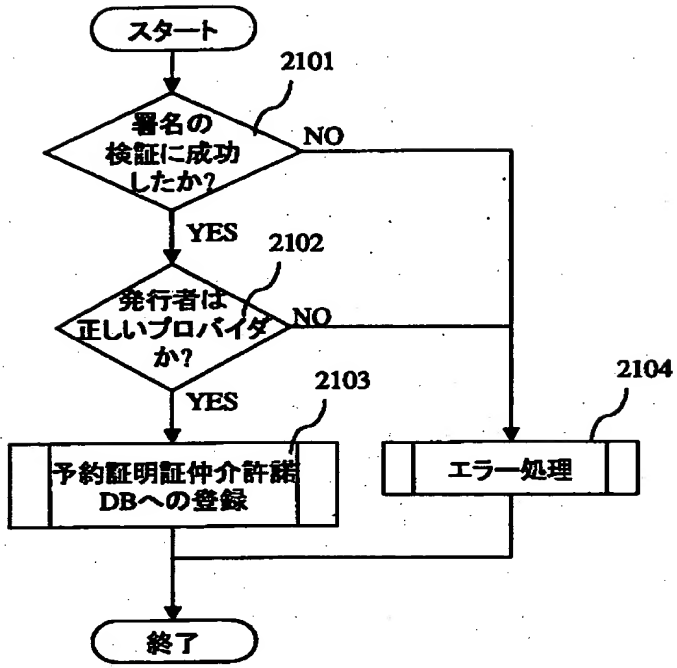
【図１９】

予約証明証仲介許諾識別子	公開鍵識別子	プロバイダ識別子	予約証明証仲介許諾	プロバイダ証明証
AGM01002	PK00001	PRV10001	FF3AC4...	FE66B...
AGM03010	PK00002	PRV10003	FF3CC2...	FEE4A...
AGM03034	PK00008	PRV10003	FFF87A...	FE7DE...
...	...	...	...	...

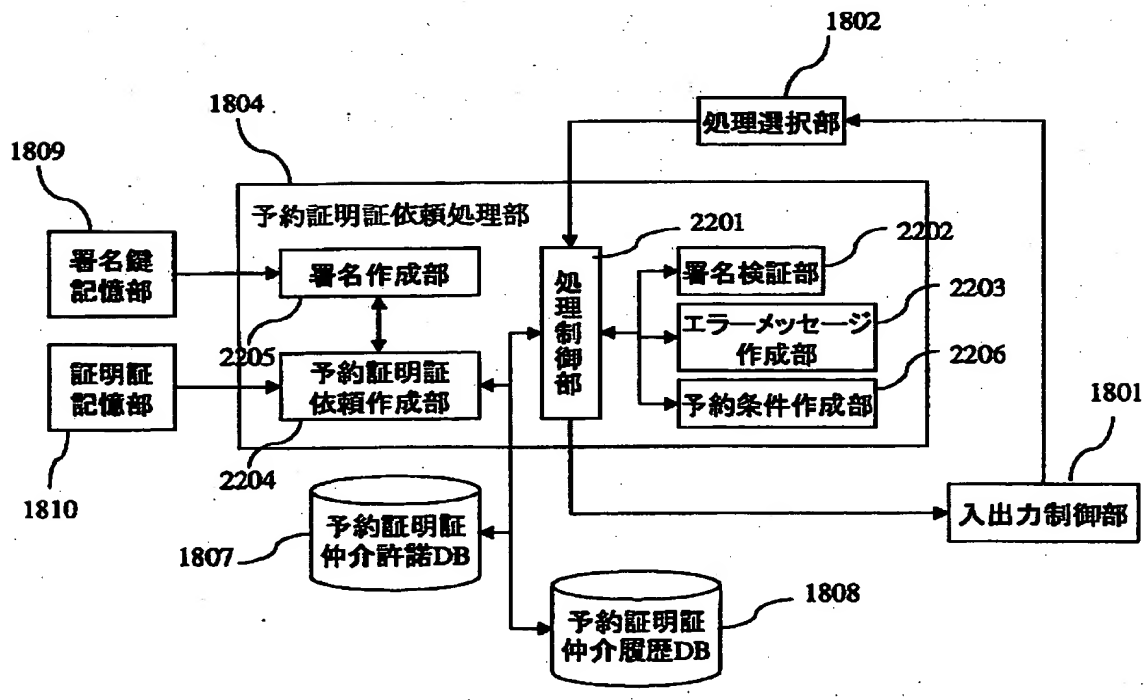
【図２０】

予約証明証識別子	公開鍵識別子	プロバイダ識別子	消費者識別子	依頼者識別子	予約条件	依頼日時	発信日時
TKT10004	PK00001	PRV10001	CNS10006	CNS10006	2F34A...	2000.2.1 10:25	2000.2.1 10:27
TKT10010	PK00008	PRV10003	CNS10003	RTL10024	44FBC...	2000.2.16 18:03	2000.2.16 18:04
	PK00001	PRV10001	CNS10012	CNS10012	5AAB1...	2000.3.1 03:54	
...	...	...	...		...	...	...

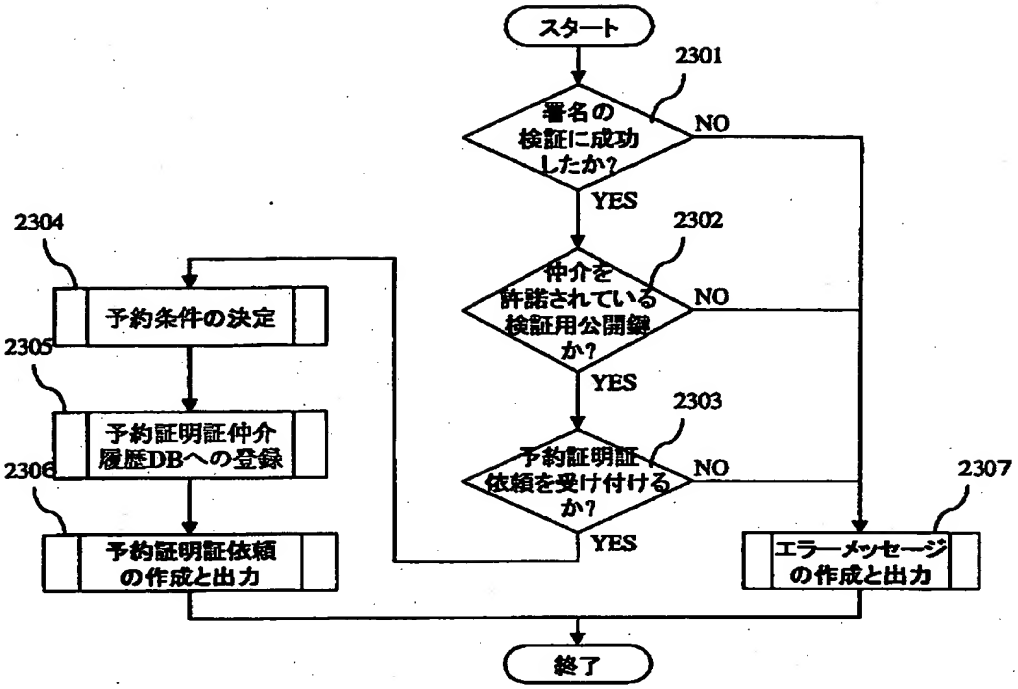
【図２１】


スタート
2101
署名の検証に成功したか?
NO
YES
2102
発行者は正しいプロバイダか?
NO
YES
2103
2104
予約証明証仲介許諾DBへの登録
エラー処理
終了

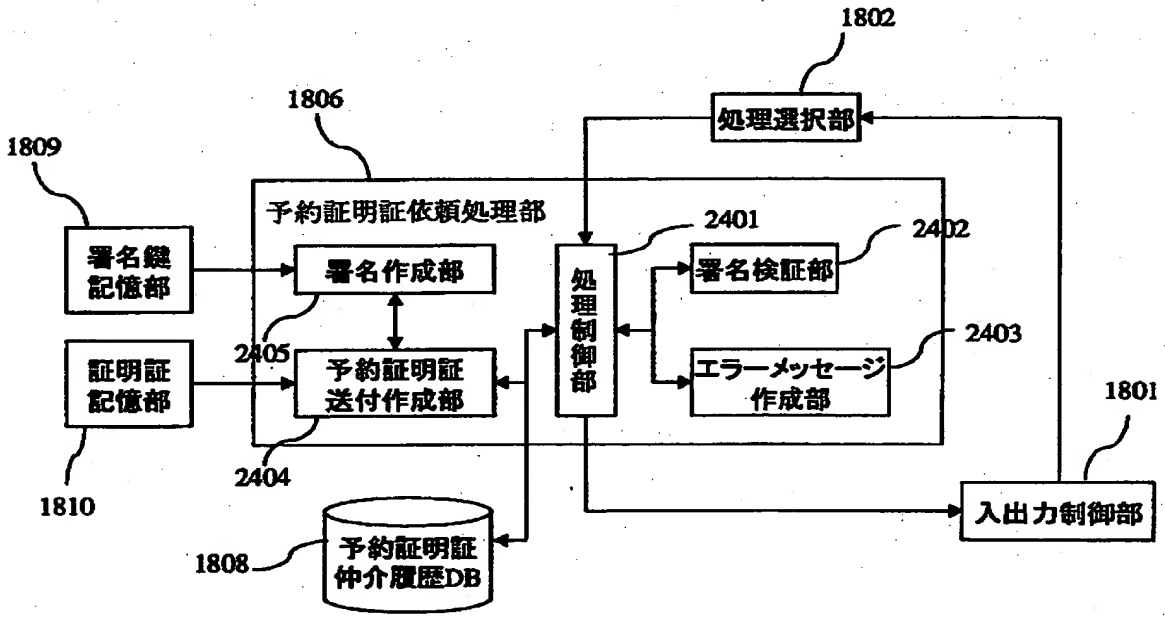
【図２２】


1802
処理選択部
1804
予約証明証依頼処理部
1809
署名鍵記憶部
署名作成部
2201
処理制御部
2202
署名検証部
2203
エラーメッセージ作成部
2206
予約条件作成部
1801
2205
証明証記憶部
予約証明証依頼作成部
2204
1810
入出力制御部
予約証明証仲介許諾DB
1807
予約証明証仲介履歴DB
1808

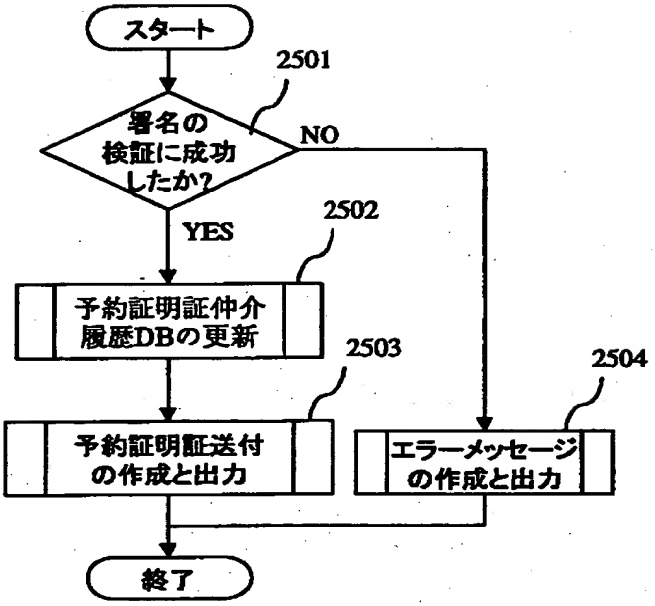
【図２３】


スタート
2301
署名の検証に成功したか?
NO
YES
2302
仲介を許諾されている検証用公開鍵か?
NO
YES
2303
予約証明証依頼を受け付けるか?
NO
YES
2304
予約条件の決定
2305
予約証明証仲介履歴DBへの登録
2306
予約証明証依頼の作成と出力
2307
エラーメッセージの作成と出力
終了

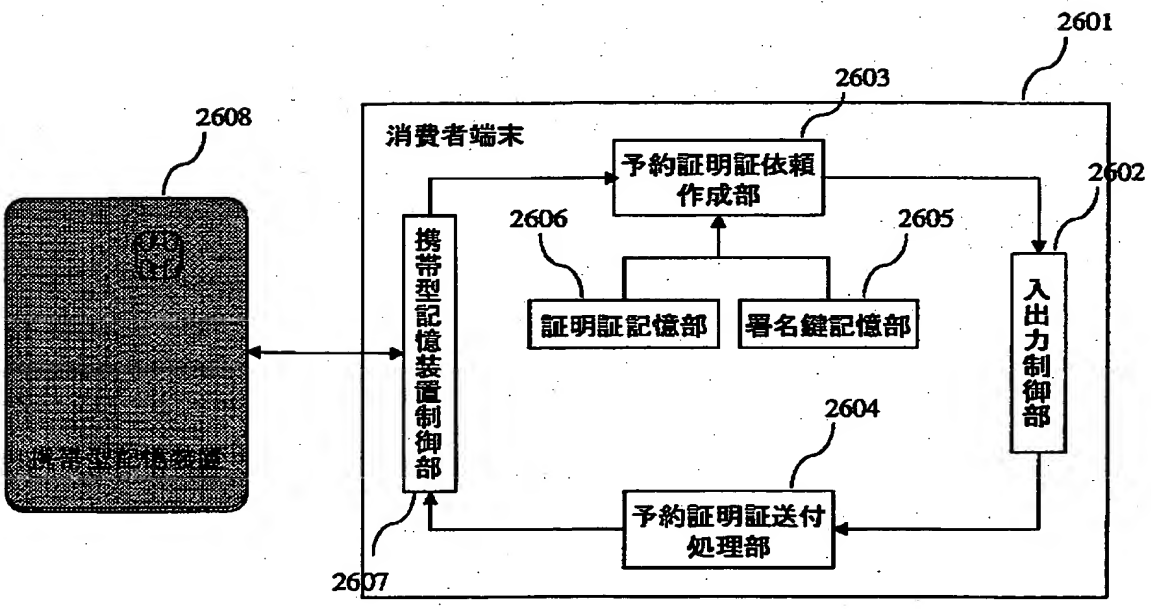
【図２４】


1802
処理選択部
1806
予約証明証依頼処理部
1809
署名鍵記憶部
署名作成部
2401
処理制御部
2402
署名検証部
2403
エラーメッセージ作成部
2405
予約証明証送付作成部
証明証記憶部
1810
2404
1808
予約証明証仲介履歴DB
1801
入出力制御部

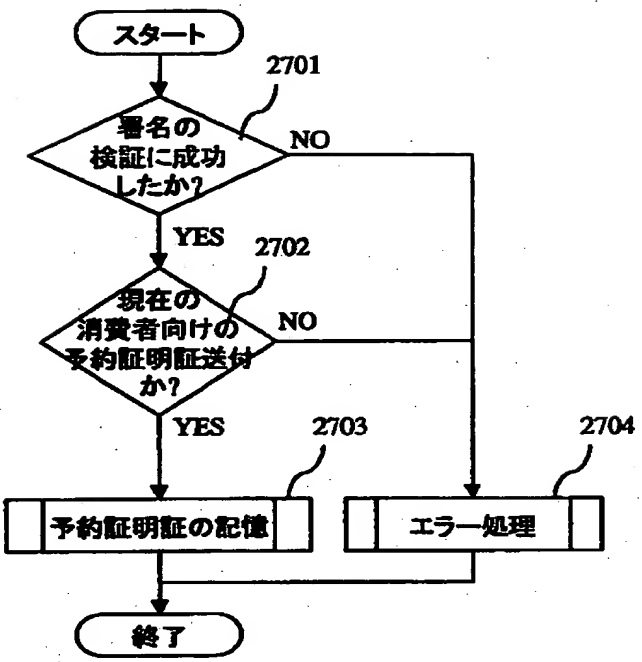
【図２５】


スタート
2501
署名の検証に成功したか?
NO
YES
2502
予約証明証仲介履歴DBの更新
2503
予約証明証送付の作成と出力
2504
エラーメッセージの作成と出力
終了

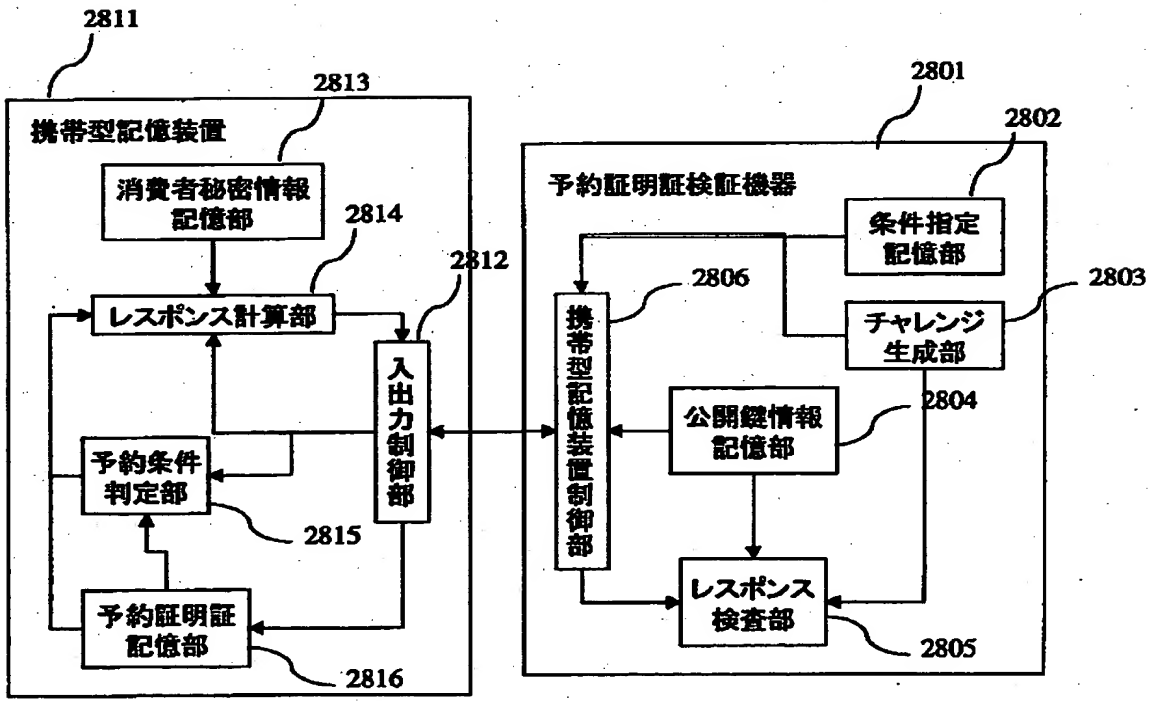
【図２６】


2601
2603
2608
消費者端末
予約証明証依頼作成部
2602
2606
2605
携帯型記憶装置制御部
証明証記憶部
署名鍵記憶部
入出力制御部
2604
予約証明証送付処理部
2607

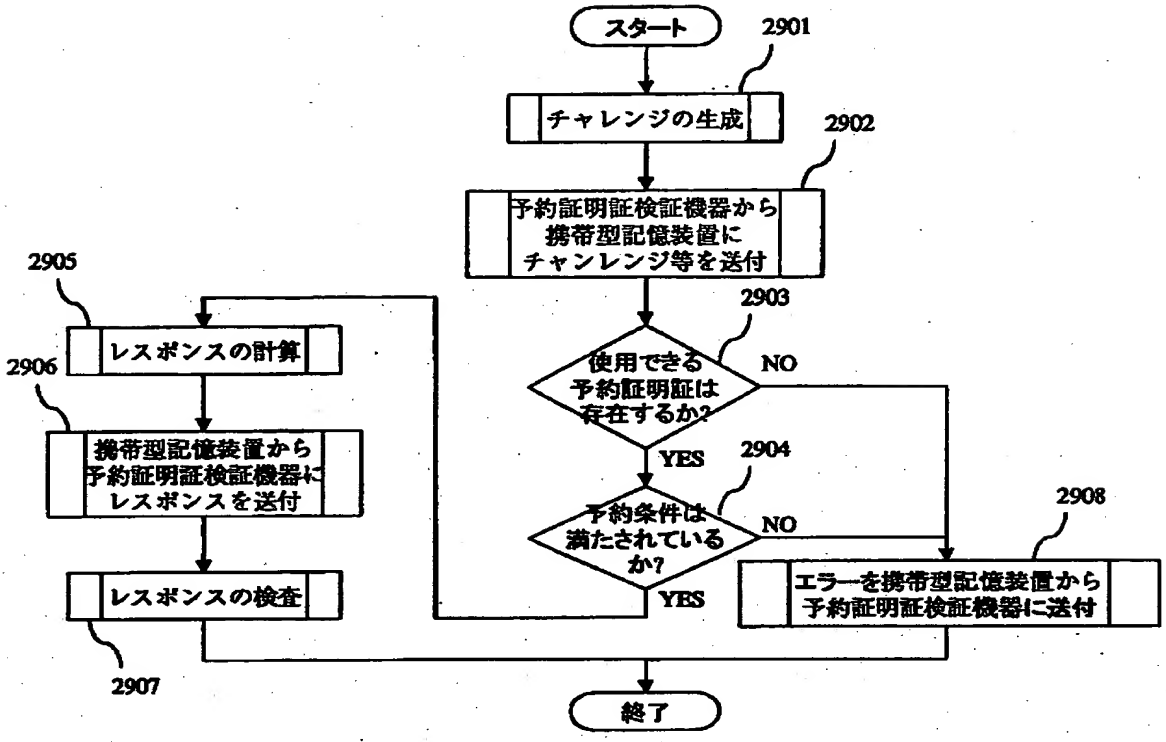
【図２７】


スタート
2701
署名の検証に成功したか?
NO
YES
2702
現在の消費者向けの予約証明証送付か?
NO
YES
2703
2704
予約証明証の記憶
エラー処理
終了

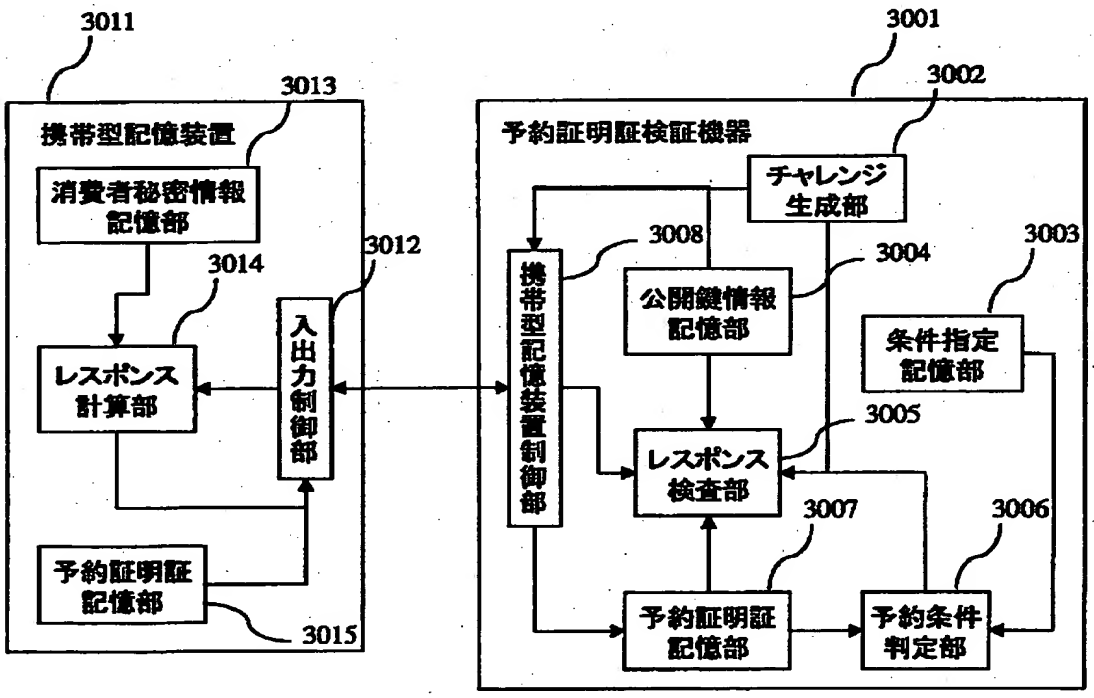
【図２８】


2811
2813
携帯型記憶装置
消費者秘密情報記憶部
2814
レスポンス計算部
2812
入出力制御部
予約条件判定部
2815
予約証明証記憶部
2816
2801
2802
予約証明証検証機器
条件指定記憶部
2806
2803
携帯型記憶装置制御部
チャレンジ生成部
公開鍵情報記憶部
2804
レスポンス検査部
2805

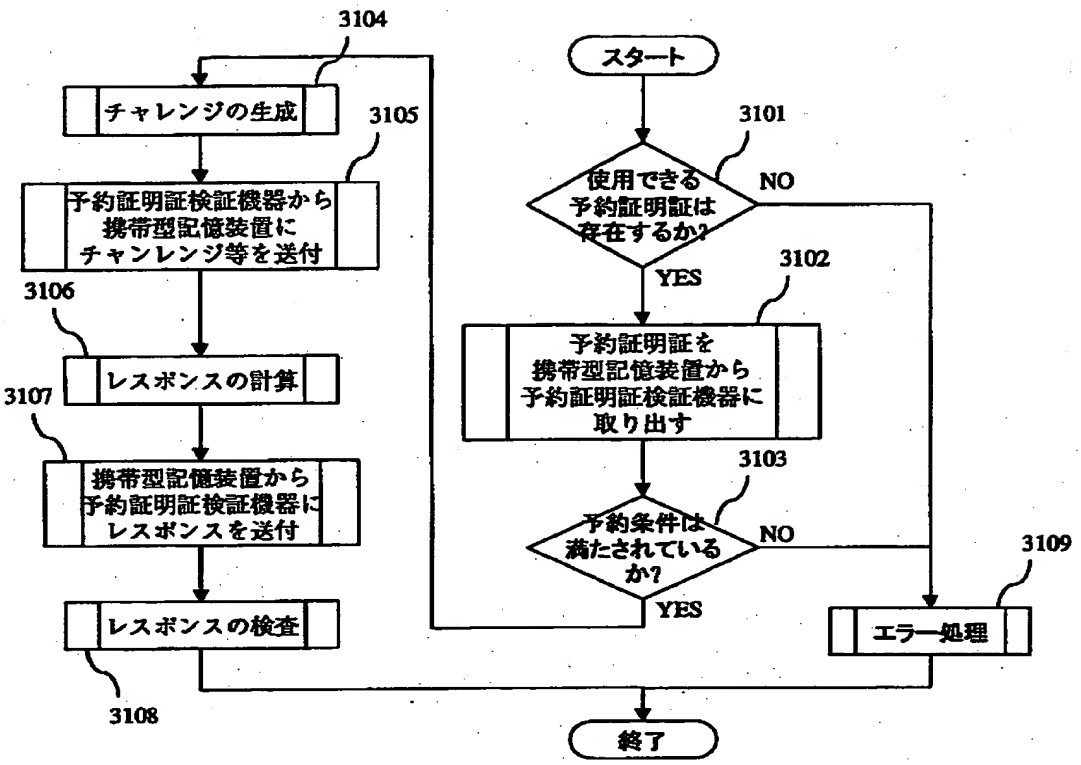
【図２９】


スタート
2901
チャレンジの生成
2902
予約証明証検証機器から
携帯型記憶装置に
チャレンジ等を送付
2903
使用できる
予約証明証は
存在するか?
NO
YES
2904
予約条件は
満たされている
か?
NO
YES
2905
レスポンスの計算
2906
携帯型記憶装置から
予約証明証検証機器に
レスポンスを送付
レスポンスの検査
2907
2908
エラーを携帯型記憶装置から
予約証明証検証機器に送付
終了

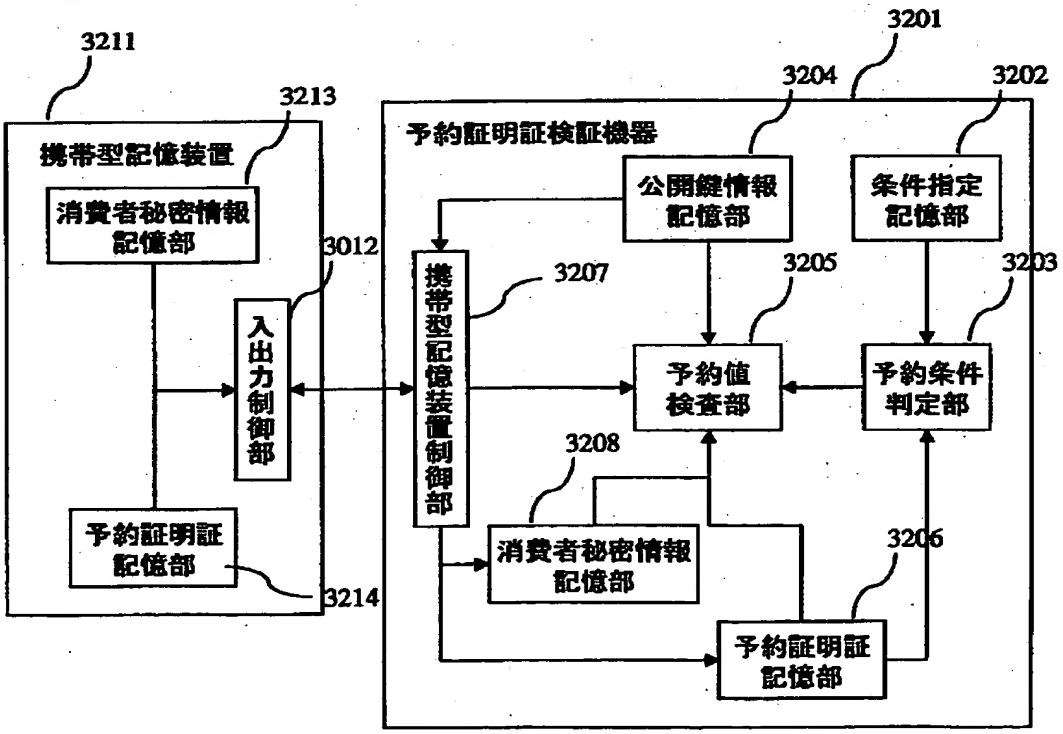
【図３０】


3011
携帯型記憶装置
3013
消費者秘密情報
記憶部
3014
レスポンス
計算部
3012
入出力制御部
予約証明証
記憶部
3015
3001
予約証明証検証機器
3002
チャレンジ
生成部
3008
携帯型記憶装置制御部
3004
公開鍵情報
記憶部
3003
条件指定
記憶部
3005
レスポンス
検査部
3007
3006
予約証明証
記憶部
予約条件
判定部

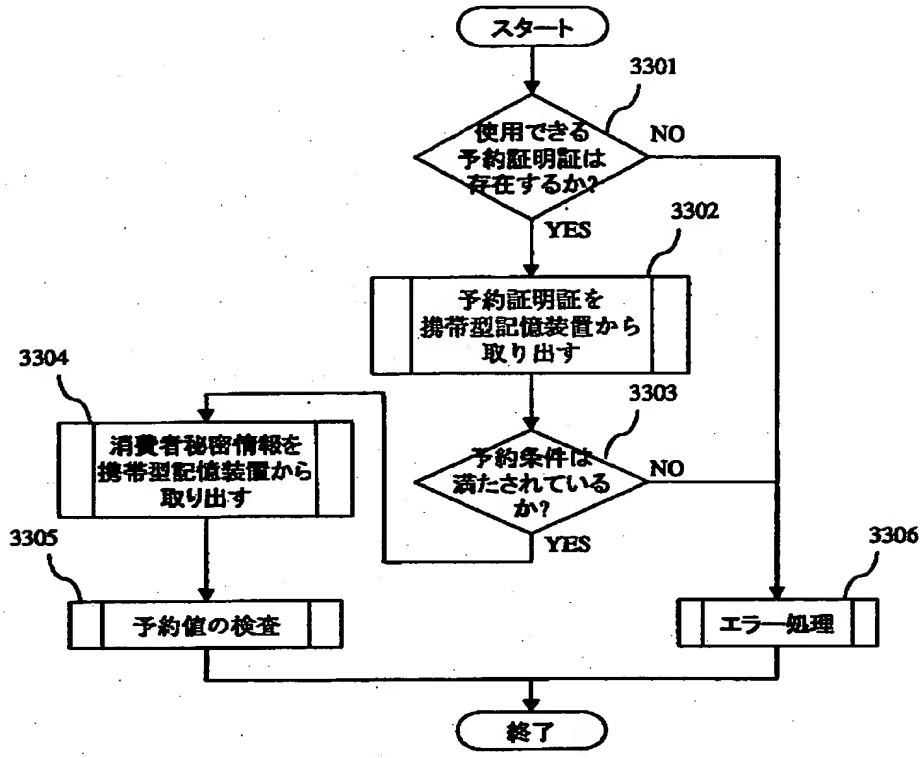
【図３１】


スタート
3101
使用できる予約証明証は存在するか?
NO
YES
3102
予約証明証を携帯型記憶装置から予約証明証検証機器に取り出す
3103
予約条件は満たされているか?
NO
YES
3104
チャレンジの生成
3105
予約証明証検証機器から携帯型記憶装置にチャンレンジ等を送付
3106
レスポンスの計算
3107
携帯型記憶装置から予約証明証検証機器にレスポンスを送付
レスポンスの検査
3108
3109
エラー処理
終了

【図３２】


3211
3213
携帯型記憶装置
消費者秘密情報記憶部
3012
入出力制御部
予約証明証記憶部
3214
3201
3204
3202
予約証明証検証機器
公開鍵情報記憶部
条件指定記憶部
3207
携帯型記憶装置制御部
3205
3203
予約値検査部
予約条件判定部
3208
消費者秘密情報記憶部
3206
予約証明証記憶部

【図３３】



【図３４】

予約証明証仲介許諾識別子	公開鍵識別子	リテーラ識別子	予約条件限定情報	有効期間開始	有効期間終了	発行日
AGM01002	PK00001	RTL10001	FF3AC4…	1999.12.1	2000.11.31	1999.12.1
AGM03010	PK00002	RTL10003	FF3CC2…	2000.1.1	2000.7.1	2000.1.1
AGM03034	PK00008	RTL10003	FFF87A…	2000.3.4	2001.3.4	2000..3.3
…	…	…	…	…	…	…

【書類名】　要約書

【要約】

【課題】　予約販売業者が自らのリソースを消費することなく予約証明証を発行できるようにする。

【解決手段】　消費者端末１０９からインターネット１０１を介してリテーラ１０３に予約が行われる。リテーラ１０３は商品や予約者に応じた予約証明証の発行を予約証明証発行センタ１０２に要求して予約証明証を受領する。消費者端末１０９はリテーラ１０３からインターネット１０１を介して予約証明証を受け取り、これを用いて正規の予約者であることをプロバイダ１０５に関連する検証機器１０６で検証を受ける。予約者は、検証が成功したら商品やサービスの提供を受けることができる。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５４９６〕

１．変更年月日　　１９９６年　５月２９日
［変更理由］　住所変更
住　所　　東京都港区赤坂二丁目１７番２２号
氏　名　　富士ゼロックス株式会社